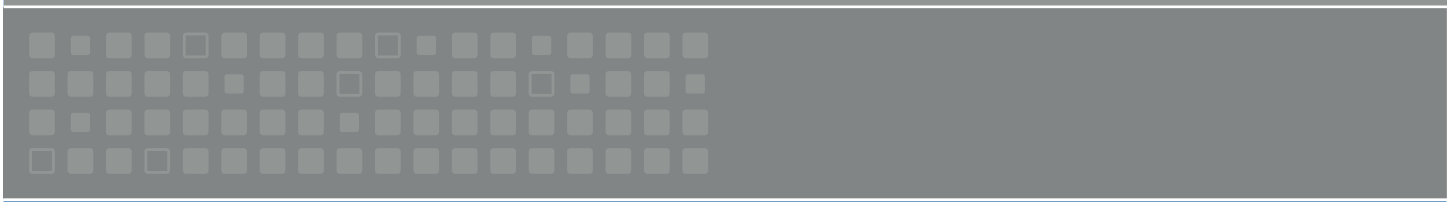
EVALUATOR'S GUIDE

VMware vCenter™ Site Recovery Manager 4.0 Evaluator's Guide



vmware®

Contents

Getting Started . . . 3
About VMware vCenter Site Recovery Manager . . . 3
About This Guide . . . 3
Intended Audience . . . 3
Assumptions . . . 3
Disaster Recovery (DR), vSphere, vCenter and Site Recovery Manager Abbreviations . . . 4
Disaster Recovery (DR) and Site Recovery Manager Terminology . . . 4
What Will Be Covered . . . 5
VMware vCenter Site Recovery Manager Evaluation Worksheet . . . 7
Help and Support During Evaluation . . . 8
VMware Contact Information . . . 8
Providing Feedback . . . 8

Overview of VMware vCenter Site Recovery Manager . . . 9

1. Site Recovery Manager Recovery Workflow . . . 12
1.1. vSphere Linked Mode . . . 12
1.2. Switch between Protected Site and Recovery Site in vSphere Client . . . 12
1.3.Replicated Storage Support (iSCSI/FC/NFS) . . . 13
1.4. Planning for BC/DR when using Site Recovery Manager . . . 13
1.5. Exercise: Setup Recovery Workflow . . . 14

2. Site Recovery Manager Alarms and Site Status Monitoring . . . 36
2.1. Exercise: Configure Site Recovery Manager Alarms . . . 37

3. Site Recovery Manager Roles and Privileges . . . 39
3.1. Exercise: Create a Site Recovery Manager Custom Role . . . 41

4. Site Recovery Manager Advanced Settings . . . 43
4.1. Optional Exercise: Change Advanced Settings . . . 43

5. Failover from Protected Site to Recovery Site . . . 45

6. Failback from Recovery Site to Protected Site . . . 47

7. Shared Recovery Site . . . 57
7.1. Use Cases of Shared Recovery Site . . . 59
7.2. Optional Exercise: Configuring Shared Recovery Site . . . 60

8. Conclusion . . . 64

vmware®

Getting Started

About VMware™ vCenter Site Recovery Manager

VMware vCenter™ Site Recovery Manager 4.0 is an extension to VMware vCenter - providing disaster recovery capabilities to VMware customers. It enables integration with array-based replication, discovery and management of replicated datastores, and automated migration of inventory from one VMware vCenter to another. Site Recovery Manager Servers coordinate the operations of the replicated storage arrays and VMware vCenter Servers at the two sites so that, as virtual machines at one site (the protected site) are shut down, virtual machines at the other site (the recovery site) start up and, using the data replicated from the protected site, assume responsibility for providing the same services. Migration of protected inventory and services from one site to the other is controlled by a recovery plan that specifies the order in which virtual machines are shut down and started up, the resource pools that they are allocated, and the networks they can access. Site Recovery Manager enables you to test a recovery plan, using a temporary copy of the replicated data, in a way that does not disrupt ongoing operations at either site.

Site Recovery Manager runs on the VMware vSphere™ platform extending the feature set to include support for NFS storage replication, protection for multiple sites by one shared recovery site, and other automation improvements.

About This Guide

The purpose of this guide is to support a self-guided, hands-on evaluation of VMware vCenter Site Recovery Manager by IT professionals who are looking to automate their disaster recovery plans by Site Recovery Manager in their VMware vSphere environment.

Intended Audience

The Site Recovery Manager 4.0 Evaluator's Guide is intended to provide Site Recovery Manager customers and evaluators a guide that walks them through the Site Recovery Manager workflow that has to be completed to allow for the successful and automated service failover from the designated Site Recovery Manager protected site to the designated Site Recovery Manager recovery site. It also provides an overview that includes the considerations and guidance to execute a failback of services from the recovery site back to the site that was originally designated as the Site Recovery Manager protected site. In addition, this guide covers the new Site Recovery Manager features – VMware vSphere support, NFS support, and shared recovery site. Evaluators can work through the exercises provided in this guide to gain a first-hand experience on operating the core and new features.

Assumptions

To successfully use this guide it is assumed that:

- VMware® ESX™/ESXi™ Server has been installed on the physical servers designated for this evaluation
- VMware vCenter™ Server 4.0 and vSphere Client ™ 4.0 have been installed in each of the Site Recovery Manager protected and recovery sites to manage the ESX Server hosts
- A multisite SAN/NFS infrastructure is in place, and setup to replicate designated VMFS/NFS datastores between the Site Recovery Manager protected and recovery sites
- The virtual machines that have been selected to be protected virtual machines for the Site Recovery Manager evaluation have been moved onto the designated replicated datastores. Virtual machines that have not been selected to be protected virtual machines for the evaluation should

[1] Site Recovery Manager 1.0 supports iSCSI and FC storage. Starting SRM 4.0, NFS is also supported.

be moved to non-replicated datastores. You can use Storage VMotion to complete the move with zero downtime

- The basic installation of Site Recovery Manager server in the Site Recovery Manager protected and recovery sites has been completed
- Storage Replication Adaptors (SRAs) have been installed at protected and recovery sites
- VMware vCenter Site Recovery Manager Plug-In has been installed and enabled on the vSphere Client instances that will be used to access the Site Recovery Manager protected and recovery sites

For detailed information regarding installation, configuration, administration, and usage of VMware vSphere and vCenter Site Recovery Manager, please refer to the online documentation:

- VMware vSphere: http://www.vmware.com/support/pubs/vs_pubs.html
- VMware vCenter Site Recovery Manager: http://www.vmware.com/products/srm/resource.html

Disaster Recovery (DR), vSphere, vCenter and Site Recovery Manager Abbreviations

The following DR, vSphere, vCenter and abbreviations are used throughout this evaluator guide:

ABBREVIATION	DESCRIPTION
BC/DR	Business Continuity and Disaster Recovery
VM	Virtual machines on a managed host
RP	vCenter Resource Pool
VMFS	Virtual Machine File System
SAN	Storage area network type datastore shared between managed hosts
NFS	Network File System

Disaster Recovery (DR) and Site Recovery Manager Terminology

The following DR and Site Recovery Manager terminology is used throughout this guide:

DR AND SRM TERMINOLOGY	DESCRIPTION
Array-based replication	Replication of virtual machines that is managed and executed by the storage subsystem itself rather than from inside the virtual machines, the vmkernel or the Service Console.
Logical unit number (LUN)	Refers to a single SCSI storage device on the SAN that can be mapped to one or more ESX Servers.
Failover	Event that occurs when the recovery site takes over operation in place of the protected site after the declaration of a disaster.
Failback	Reversal of failover, returning IT operations to the primary site.
Datastore	Storage for the managed host.
Host	vCenter managed hosts.
SRM Server	Short form for VMware vCenter Site Recovery Manager Server. SRM Server extends VMware vCenter to provide disaster recovery capabilities for VMware customers. It enables integration with array-based replication, discovery and management of replicated datastores, and automated migration of VMware inventory from one vCenter to another.

[2] Note that virtual machines that are added or moved to a replicated datastore after the protection group has been added will need to be configured for protection explicitly.

[3] Note that migrating a previously protected virtual machine to a non-replicated datastore does not automatically remove protection. Explicit configuration is needed.

Protected VM	A VM that is protected by SRM and it is located on a replicated datastore.
Un-protected VM	A VM that is not protected by SRM and it is located on a non replicated datastore.
Protected site	The site that contains the protected VMs.
Recovery site	The site that contains the replicated protected VMs from the protected site.
Datastore group	Replicated datastores containing complete sets of protected VM.
Protection group	A group of VMs that will be failed over together to the recovery site during test or recovery.
Storage Replication Adapter (SRA)	Enables SRM to interact with a storage array.
Placeholder VM	An artifact in the recovery site vCenter inventory that represents a protected VM from the protected site vCenter.
Inventory mappings	Associations between resource pools, VM folders, networks at the protected site and their destination counterparts at the recovery site.
Recovery plan	Contains the complete set of steps needed to recover (or test recovery of) the protected VMs in one or more protection groups.

What Will Be Covered

This guide provides you with an overview of the Site Recovery Manager features and capabilities:

1. Site Recovery Manager Recovery Workflow
2. Site Recovery Manager Alarms and Site Status Monitoring
3. Site Recovery Manager Roles and Privileges
4. Site Recovery Manager Advanced Settings
5. Failover from Protected Site to Recovery Site
6. Failback from Recovery Site to Protected Site
7. Shared Recovery Site

It is highly recommended that you work through the exercises in the section to experience the Site Recovery Manager features and capabilities first-hand. For **changing advanced setting, failover, failback,** and **shared recovery site**, you can simply read through the details provided in the corresponding sections listed above if you decide not to go through the real operations. The exercises include:

[4] Note that the real time spent on each exercise is dependent on the specifics of your environment. These are time estimates that were gathered from working in this test environment that has a small number of virtual machines

CATEGORY	FEATURES	WHAT WILL BE COVERED	TIME ESTIMATES [4]
SRM Recovery Workflow	**Recovery Workflow Automation**	Set up Recovery Workflow 1. Set up site-pairing 2. Set up Array Managers for the replicated datastore 3. Set up inventory mappings 4. Set up protection group 5. Set up recovery plan 6. Configure IP customization 7. Trigger a test recovery	60 minutes
SRM Alarms	**Configure action for a SRM Alarm**	Configure action for alarm 'Remote Site Down' 1. Configure alarm action to send out notification email.	10 minutes
SRM Roles	**Custom Role Creation**	Create a SRM Custom Role 1. Create a SRM custom role with SRM specific privileges.	10 minutes
SRM Advanced Settings (Optional)	**Change Advanced Settings**	Change Advanced Settings (Exercise is optional) 1. Change one of the advanced settings, e.g. SanProvider.CommandTimeout.	20 minutes
SRM failover from Protected Site to Recovery Site (Optional)	**Failover**	Details of failover operations (Exercise is optional)	30 minutes
SRM failover from Recovery Site to Protected Site (Optional)	**Failover**	Details of failback operations (Exercise is optional)	90 minutes
Shared Recovery Site (Optional)	**Configure Shared Recovery Site**	Protect 2 sites by a shared recovery site (Exercise is optional) Pre-requisite: Two protected sites with separate vCenter servers, one recovery site with another vCenter server. 1. Install a SRM instance using a custom switch on both the protected and recovery sites with custom SRM plug-in ID and same authentication method. 2. Pair sites. 3. Install a SRM instance on another protected site and another SRM instance on the recovery site. Repeat the procedures in step 1 and step 2.	30 minutes

VMware vCenter Site Recovery Manager Evaluation Worksheet

You can use the worksheet below to organize your evaluation process.

HARDWARE CHECKLIST	
Physical Servers	

SOFTWARE CHECKLIST	
VMware vSphere ESX/ESXi Server	
VMware vCenter Server (and associated database)	
VMware vSphere Client	
VMware vCenter Site Recovery Manager Server (and associated database)	
VMware vCenter Site Recovery Manager Plug-In	
Storage Replication Adaptor (SRA) - Storage vendor specific	

After you have successfully installed the VMware vSphere and vCenter Site Recovery Manager software components on your hardware, you can proceed to perform the evaluation of VMware vCenter Site Recovery Manager. For each scenario, you can use the corresponding checklist below to ensure that you are following the proper sequence.

EVALUATION EXERCISES	
SRM Recovery Workflow	
SRM Roles and Privileges	
SRM Alarms and Site Status Monitoring	
SRM Advanced Settings (Optional)	
Failover from Protected Site to Recovery Site (Optional)	
Failback from Recovery Site to Protected Site (Optional)	
Shared Recovery Site (Optional)	

Help and Support During Evaluation

This guide is intended to provide an overview of the steps required to ensure a successful evaluation of VMware vCenter Site Recovery Manager. It is not meant to substitute product documentation. Please refer to the online product documentation for Site Recovery Manager for more detailed information (See below for links). You may also consult the online Knowledge Base if you have any additional questions. Should you require further assistance, please contact a VMware sales representative or channel partner.

VMware vCenter Site Recovery Manager Resources

Product Resources: http://www.vmware.com/products/srm/resource.html

Product Community: http://www.vmware.com/products/srm/community.html

VMware vCenter Site Recovery Manager Administrator's Guide: http://www.vmware.com/pdf/srm-admin.pdf

Automating Network Setting Changes and DNS Updates on Recovery Site Using VMware vCenter Site Recovery Manager: http://viops.vmware.com/home/docs/DOC-1491

Adding a DNS Update Step to a Recovery Plan: http://www.vmware.com/pdf/srm_dns_updater.pdf

Installing, Configuring and Using Shared Recovery Site Support: http://www.vmware.com/pdf/srm_shared_recovery.pdf

VMware vCenter Site Recovery Manager Compatibility Matrixes: http://www.vmware.com/pdf/srm_compat_matrix_4_0.pdf

VMware vSphere and vCenter Resources

Product Documentation: http://www.vmware.com/support/pubs/

vSphere Basic System Administration Guide: http://www.vmware.com/pdf/vsphere4/r40/vsp_40_admin_guide.pdf

Online Support: http://www.vmware.com/support/

Support Offerings: http://www.vmware.com/support/services

Education Services: http://mylearn1.vmware.com/mgrreg/index.cfm

Support Knowledge Base: http://kb.vmware.com

VMware Contact Information

For additional information, or to purchase VMware vSphere and VMware vCenter Site Recovery Manager, VMware's global network of solution providers are ready to assist you. If you would like to contact VMware directly, you can reach a sales representative at 1-877-4VMWARE (650-475-5000 outside North America) or email sales@vmware.com. When emailing, please include the state, country, and company name from which you are inquiring. You can also visit: http://www.vmware.com/vmwarestore/.

Providing Feedback

Your feedback is appreciated on the material included in this guide. In particular, any guidance on the following topics would be extremely helpful:

- How useful was the information in this guide?
- What other specific topics would you like to see covered?
- Overall, how would you rate this guide?

Please send your feedback to the following address: tmdocfeedback@vmware.com, with "VMware vCenter Site Recovery Manager 4.0 Evaluator's Guide" in the subject line. Thank you for your help in making these guides a valuable resource.

Overview of VMware vCenter Site Recovery Manager

VMware vCenter Site Recovery Manager provides business continuity and disaster recovery protection for virtual environments. Protection can extend from individual replicated datastores to an entire virtual site. VMware's virtualization of the data center offers advantages that can be applied to business continuity and disaster recovery, including:

- The entire state of a virtual machine (memory, disk images, I/O, and device state) is encapsulated. Encapsulation enables the state of a virtual machine to be saved to a file. Saving the state of a virtual machine to a file allows the transfer of an entire virtual machine to another host.
- Hardware independence eliminates the need for a complete replication of hardware at the recovery site. Hardware running ESX at one site can provide business continuity and disaster recovery protection for hardware running ESX at another site. This eliminates the cost of purchasing and maintaining a system that sits idle until disaster strikes.
- Hardware independence allows an image of the system at the protected site to boot from disk at the recovery site in minutes or hours instead of days.

Site Recovery Manager leverages array-based replication between a protected site and a recovery site. The workflow that is built into Site Recovery Manager automatically discovers which datastores are setup for replication between the protected and recovery sites. Site Recovery Manager can be configured to support bi-directional protection between two sites.

Site Recovery Manager provides protection for the operating systems and applications encapsulated by the virtual machines running on ESX. A Site Recovery Manager server must be installed at the protected site and at the recovery site. The protected and recovery sites must each be managed by their own vCenter Server. The Site Recovery Manager server uses the extensibility of the vCenter Server to provide:

- Access control
- Authorization
- Custom events
- Event-triggered alarms

Site Recovery Manager Prerequisites

Site Recovery Manager has the following prerequisites:

- A vCenter server installed at the protected site.
- A vCenter server installed at the recovery site.
- Pre-configured array-based replication between the protected site and the recovery site.
- Network configuration that allows TCP connectivity between Site Recovery Manager servers and vCenter servers.
- An Oracle or SQL Server database that uses ODBC for connectivity in the protected site and in the recovery site.
- A Site Recovery Manager license installed at the protected site and the recovery site.

Site Recovery Manager Configuration and Protection

The following workflows for the protected and recovery sites accomplish setup and configuration. Site Recovery Manager is installed as a plugin into a VMware vSphere Client. Site Recovery Manager uses the VMware vSphere Client as the User Interface (UI). The Site Recovery Manager UI is accessed by clicking on the **Site Recovery** icon on the vSphere Client Home page and is used for the setup of the Site Recovery Manager workflows, recovery plan testing as well as services failover from the protected site to the recovery site.

It is important to complete the workflows in the order they are presented in this guide.

The recovery site configuration workflow involves the following activities:

- The user installs the Site Recovery Manager server.
- The user installs the SRA and restarts Site Recovery Manager service.
- The user installs the Site Recovery Manager plugin into the vSphere Client.

The protection site configuration workflow involves the following activities:

- The user installs the Site Recovery Manager server.
- The user installs the SRA and restarts Site Recovery Manager service.
- If a different VMware vSphere Client is used to access the protected and recovery sites, the user installs the Site Recovery Manager plugin into the VMware vSphere Client. Otherwise this activity can be skipped.
- Security certificates are established between the Site Recovery Manager servers and the VMware vCenter servers.
- The user pairs the Site Recovery Manager servers at the protected and recovery sites.
- Site Recovery Manager identifies available arrays and replicated datastores and determines the datastore groups.

The protection site protection workflow involves the following activities:

- Using the Inventory Mapping interface, the user maps the networks, resource pools, and virtual machine folders in the protected site to their counterparts in the recovery site.
- The user creates protection groups from the datastore groups discovered by Site Recovery Manager.
- For each protected virtual machine, the user can override default values.

The recovery site protection workflow involves the following activities:

- The user creates the recovery plan.
- Site Recovery Manager creates the recovery plan steps.
- Optionally the user has the ability to customize the recovery plan.

Failover and Testing

Site Recovery Manager automates many of the tasks required at failover. With the push of one button, Site Recovery Manager:

- Shuts down the protected virtual machines if there is connectivity between sites and they are online.
- Suspends data replication and Read/Write enable the replica devices.
- Re-scans the ESX servers at the recovery site to find iSCSI and FC devices and mounts replicas of NFS volumes.
- Registers the replicated virtual machines.
- Suspends non-essential virtual machines at the recovery site if specified to free up resources for the protected virtual machines being failed over.

- Completes power-up of replicated protected virtual machines in accordance with the recovery plan.
- Provides a report of failover results.

Site Recovery Manager does not require production system downtime to run tests. This means you can test often to ensure that you are protected in case of a disaster. For testing, Site Recovery Manager:

- Creates a test environment that includes network and storage infrastructure that is isolated from the production environment.
- Re-scans the ESX servers at the recovery site to find iSCSI and FC devices and mounts replicas of NFS volumes.
- Registers the replicated virtual machines.
- Suspends non-essential virtual machines at the recovery site if specified to free up resources for the protected virtual machines being failed over.
- Completes power-up of replicated protected virtual machines in accordance with the recovery plan.
- Resets everything in preparation for a failover or next scheduled Site Recovery Manager Test.
- Provides a report of test results.

[5] SRM does not perform the rescan if the replicated store is NFS based.

1. Site Recovery Manager Recovery Workflow

1.1. vSphere Linked Mode

Site Recovery Manager 4.0 is fully compatible with VMware vSphere. Multiple VMware vCenter Servers can be joined together using Linked Mode to allow them to be managed using a single VMware vSphere Client connection. Taking advantage of VMware vSphere Linked Mode, you can view the virtual inventories of both the protected and the recovery site in a single pane of glass. See Figure 1. Refer to the VMware vSphere Basic System Administration Guide (http://www.vmware.com/pdf/vsphere4/r40/vsp_40_admin_guide.pdf) for more information about vSphere Linked Mode.

Figure 1: Inventory View in vSphere Linked Mode

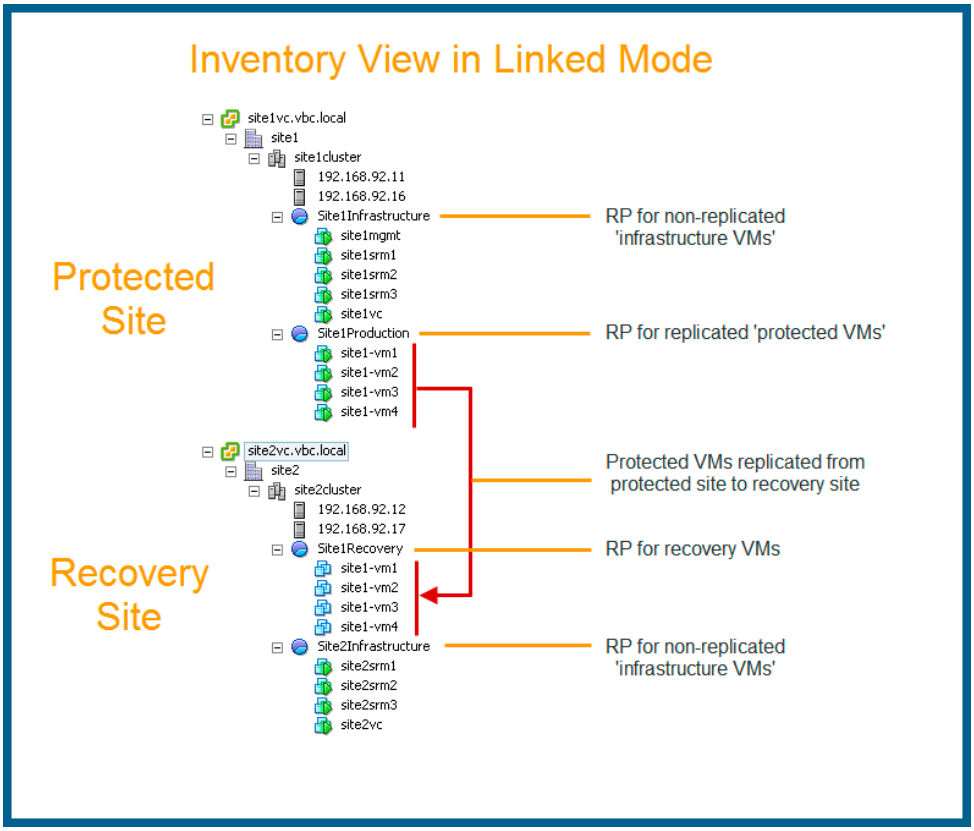
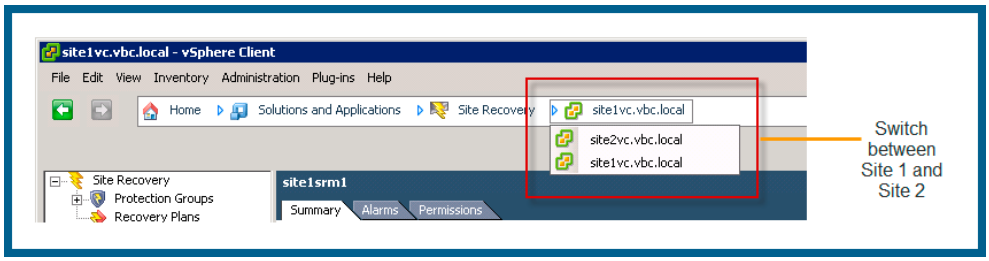


Figure 1 illustrates the inventory view of both the protected site and the recovery site in the lab environment in a single pane of glass. Both the protected site and the recovery site have divided their resources into two resource pools – one for infrastructure virtual machines, and another for production or recovery. The infrastructure virtual machines are generally bound to the data center and thus are not replicated. The protected virtual machines host application type services, and these are the services that need to be made available to the business at time of disaster.

1.2. Switch between Protected Site and Recovery Site in vSphere Client

With Site Recovery Manager 4.0, you no longer have to use two separate vSphere Clients to connect to each site separately. Site Recovery Manager 4.0 allows you to easily switch between the protected site and recovery site within the same Site Recovery Manager UI via a drop-down menu. See Figure 2.

Figure 2: Switch between protected site and recovery site



1.3.Replicated Storage Support (iSCSI/FC/NFS)

Site Recovery Manager 4.0 expands storage support from iSCSI and Fiber Channel arrays to also include replicated NFS arrays. Configuration of NFS arrays works the same way as the configurations of FC and iSCSI storage arrays[6]. You can use your replicated NFS datastores in conjunction with Site Recovery Manager 4.0 to provide disaster recovery protection for your virtual environment. Refer to http://www.vmware.com/pdf/srm_compat_matrix_4_0.pdf for a list of Site Recovery Manager compatible storage providers.

1.4. Planning for BC/DR when using Site Recovery Manager

Site planning and preparation at the protected site involves the following:

- Identify which virtual machines will be designated as protected virtual machines.
  - **site1-vm1** through **site1-vm4** in this lab (See Figure 1).
- Identify which virtual machines will be designated as un-protected virtual machines
  - **Site Recovery Manager servers and vCenter servers[7]** (See Figure 1).
- Determine which datastores to hold the protected virtual machines. If existing datastores will be used for the protected virtual machines, identify which datastores need to be configured for replication, otherwise provision the required number of new datastores to host the protected virtual machines. Working with your storage team to ensure all the datastores that will host protected virtual machines are configured for replication. Refer to the SRA configuration guide for details on replication configuration.
- Move all the designated protected virtual machines onto the replicated datastores. Storage VMotion can be used to complete the relocation of the protected virtual machines with zero service downtime.
  If possible ensure there are only protected virtual machines on the datastores that are being replicated from the protected site to the recovery site.

Site planning and preparation at the recovery site involves the following:

- Ensure that you have sufficient resources (i.e. CPU, memory and network) at the recovery site for the recovered virtual machines to utilize.

[6] In case of NFS, SRM does not perform host rescan during recovery.
[7] Other infrastructure virtual machines may include Active Directory server, DNS Server, and Print server.

1.5. Exercise: Setup Recovery Workflow

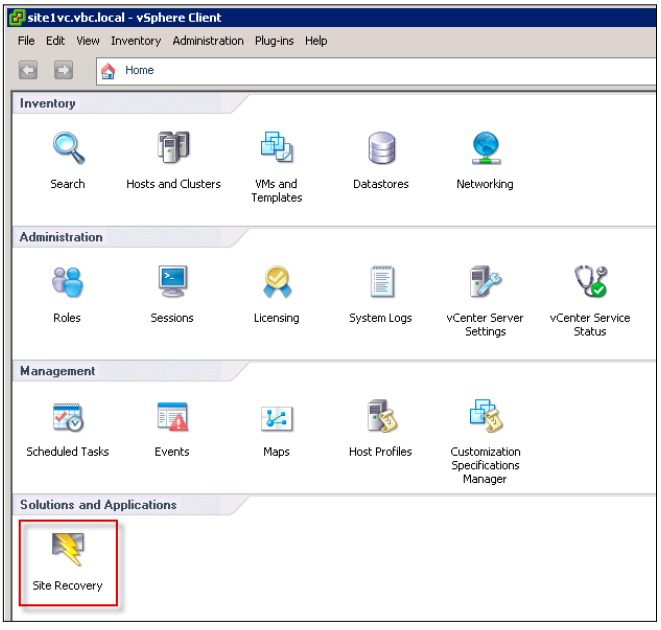
SRM Recovery Workflow	**Recovery Workflow Automation**	Set up Recovery Workflow 1. Set up site-pairing 2. Set up Array Managers for the replicated datastore 3. Set up inventory mappings 4. Set up protection group 5. Set up recovery plan 6. Configure IP customization 7. Trigger a test recovery	60 minutes

Step 1: Set up connection pairing

To set up connection pairing:

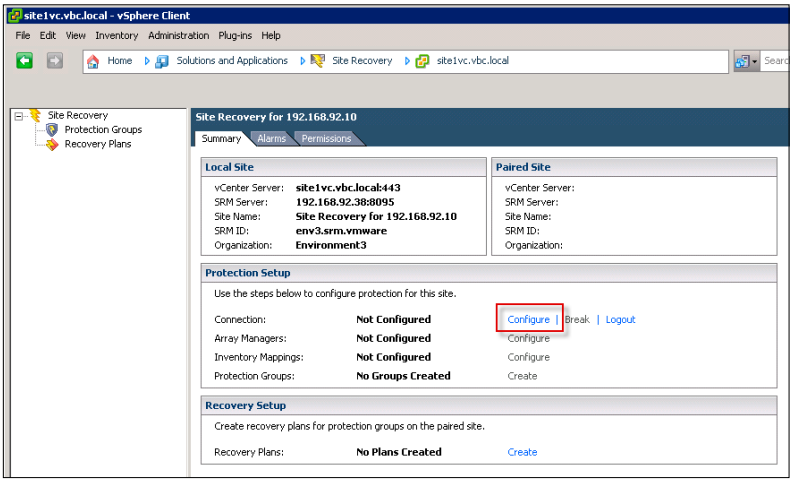
1. Open a vSphere Client and connect to the vCenter server at the protected site.
2. Log in as a vSphere administrator.
   NOTE: The recovery site must be the replication target of arrays managed by the SRA at the protected site.
3. Click the Site **Recovery icon** on the vSphere Client Home page.

Figure 3: vSphere Client Home page – Site Recovery icon



4. In the **Protection Setup** area of the **Summary** window, navigate to the **Connection** line and click **Configure**.

Figure 4: Configure connection pairing of protected and recovery sites

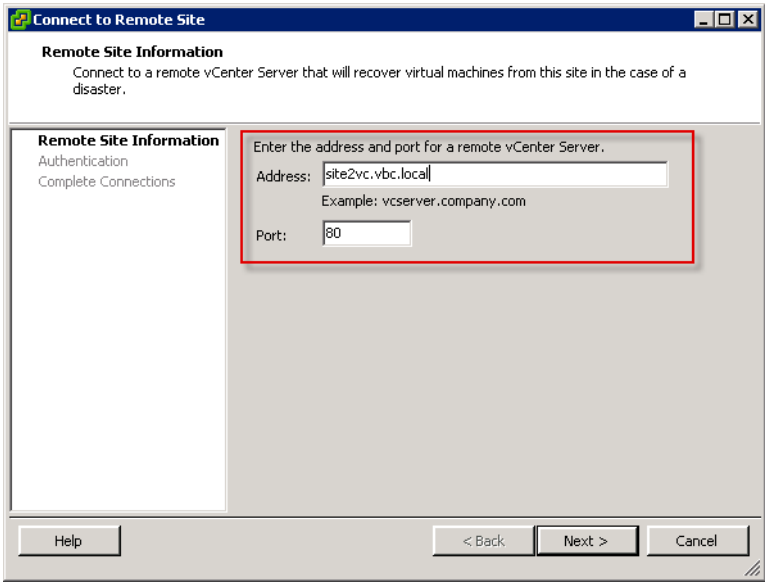

site1vc.vbc.local - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Solutions and Applications Site Recovery site1vc.vbc.local
Site Recovery
Protection Groups
Recovery Plans
Site Recovery for 192.168.92.10
Summary Alarms Permissions
Local Site
vCenter Server: site1vc.vbc.local:443
SRM Server: 192.168.92.38:8095
Site Name: Site Recovery for 192.168.92.10
SRM ID: env3.srm.vmware
Organization: Environment3
Paired Site
vCenter Server:
SRM Server:
Site Name:
SRM ID:
Organization:
Protection Setup
Use the steps below to configure protection for this site.
Connection: Not Configured Configure | Break | Logout
Array Managers: Not Configured Configure
Inventory Mappings: Not Configured Configure
Protection Groups: No Groups Created Create
Recovery Setup
Create recovery plans for protection groups on the paired site.
Recovery Plans: No Plans Created Create

5. On the **Remote Site Information** page, type the IP address or hostname of the vCenter server at the recovery site and click **Next**.

   NOTE: If you are using credential-based authentication, you must supply exactly the same information here that you entered when installing the Site Recovery Manager server. If you entered an IP address in that step, enter it again here. If you entered a hostname in that step, enter it here in exactly the same way.

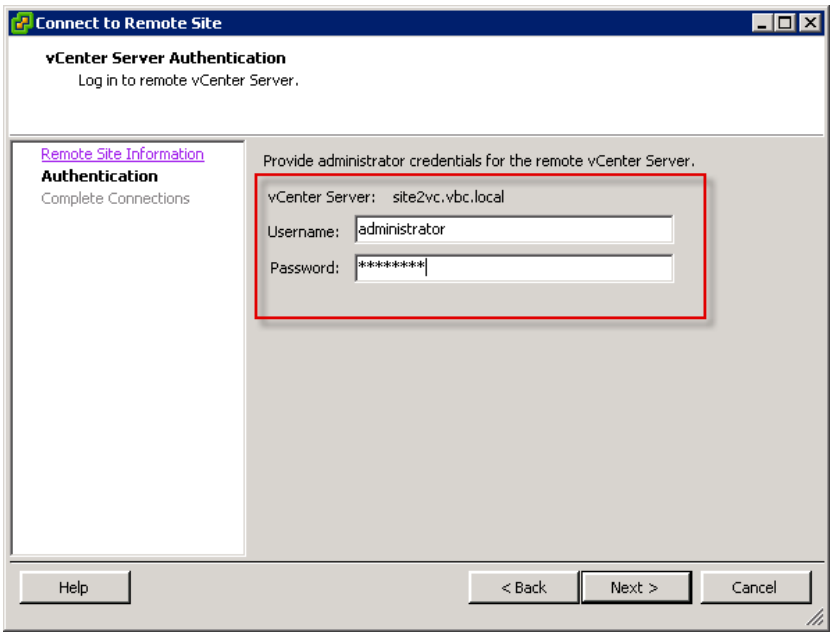
   Port 80 is provided as the default to use for the initial connection to the remote site. After the initial HTTP connection is made, the two sites establish an SSL connection over port 80 to use for subsequent connections.

Figure 5: Enter remote site information


Connect to Remote Site
Remote Site Information
Connect to a remote vCenter Server that will recover virtual machines from this site in the case of a disaster.
Remote Site Information
Authentication
Complete Connections
Enter the address and port for a remote vCenter Server.
Address: site2vc.vbc.local
Example: vcserver.company.com
Port: 80
Help
< Back
Next >
Cancel

6. On the **vCenter Server Authentication** page, provide the appropriate vCenter administrator credentials (username and password) for the remote site and click **Next**.

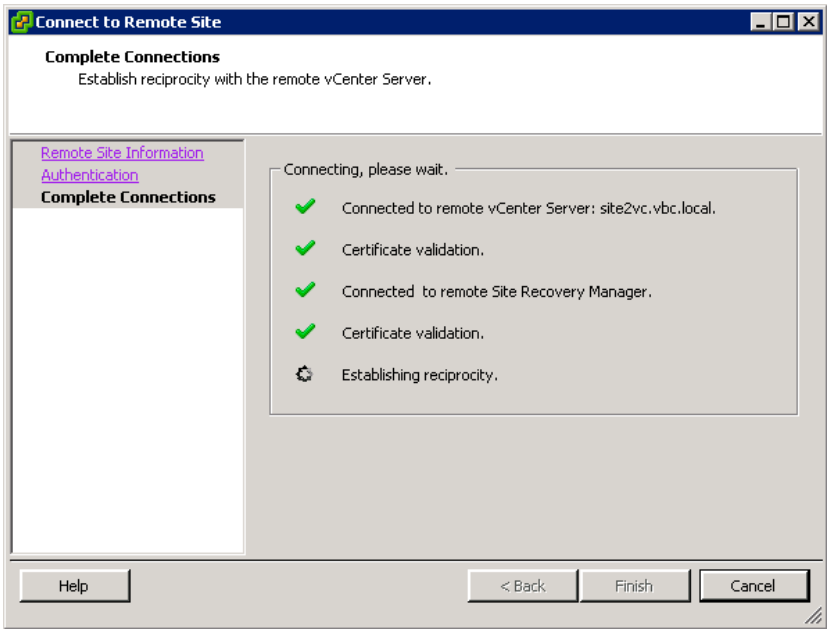
Figure 6: Enter vCenter server authentication information



If you are using credential-based authentication, you must supply exactly the same information here that you entered when installing the Site Recovery Manager server.

7. On the **Complete Connections** page, click **Finish** after all of the site paring steps have completed successfully.

Figure 7: Complete connection pairing



The Site Recovery Manager and vCenter servers at the protected and recovery sites are connected. Connection information is saved in the Site Recovery Manager databases, and persists across logins and host restarts.

Step 2: Set up array managers[8]

After you have connected the protected and recovery sites, you must configure their respective array managers so that Site Recovery Manager can discover replicated devices, compute datastore groups, and initiate storage operations.

The array manager configuration wizard leads you through a number of steps:

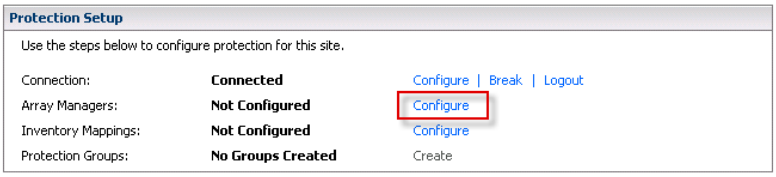
- You provide Site Recovery Manager with connection information and credentials (if needed) for array management systems at the protected and recovery sites.
- Site Recovery Manager verifies that it can connect to arrays at both sites.
- Site Recovery Manager verifies that it can discover replicated storage devices on these arrays and identify the datastores that they support.
- Site Recovery Manager computes datastore groups based on virtual machine storage layout and any consistency groups defined by the storage array.

When the configuration process is complete, the wizard presents a list of datastore groups. You typically configure array managers only once, after you have connected the protected and recovery sites. You do not need to reconfigure them unless array manager connection information or credentials have changed, or you want to use a different set of arrays.

Procedure

1. Open a vSphere Client and connect to the vCenter server at the protected site. Log in as a vSphere administrator.
2. Click the **Site Recovery** icon on the vSphere Client Home page.
3. In the **Protection Setup** area of the **Summary** window, navigate to the **Array Managers** line and click **Configure**.

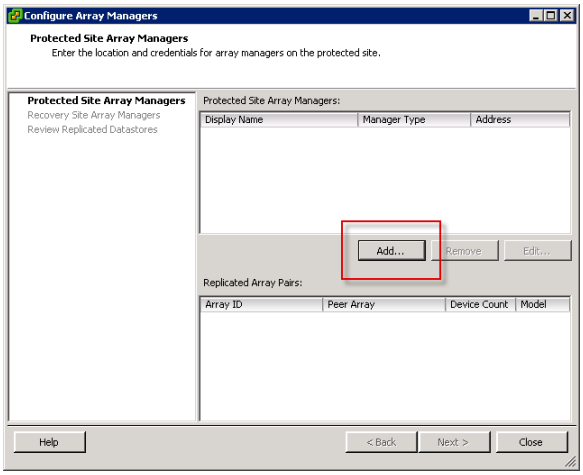
Figure 8: Configure array mangers



[8] The example here uses a replicated NFS store. You may have a different storage device type (e.g. iSCSI or FC). In this case, you may see a slight variation of input parameters depending on the storage device type. Yet the general workflow should still be similar.

4. On the **Protected Site Array Managers** page of the Configure Array Managers wizard, click **Add**.

Figure 9: Add array manager for protected site



5. Make sure that the SRA that you want Site Recovery Manager to use appears in the **Manager Type** field.

   If more than one SRA has been installed on the Site Recovery Manager server host, click the drop-down arrow and select the manager type you want to use. If no manager type is displayed, no SRA has been installed on the Site Recovery Manager host. For more information, see *"Install the Storage Replication Adapters"* in chapter 2 of Site Recovery Manager 4.0 Administration Guide.

   For this example, "EMC Celerra Replicator" was used.

6. Type a name for the array in the **Display Name** field of the Add Array Manager window. Use any descriptive name that makes it easy for you to identify the storage associated with this array manager

   For this example "NFS_SRA_Site 1" was used.

7. Fill in the remaining fields of the Add Array Manager window.

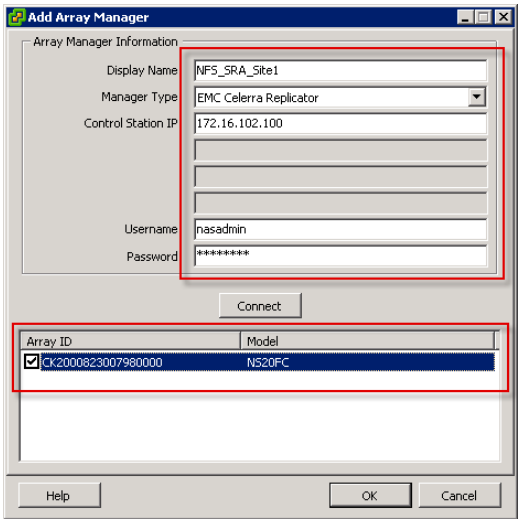
   These fields are defined by the SRA. For more information about how to fill them in, see the documentation provided by your SRA vendor.

8. Click **Connect** to validate the information you supplied and get the list of arrays that the selected array manager has discovered. All discovered arrays are selected. Clear the selection of any array that you do not want Site Recovery Manager to use.

9. Click **OK**.

   The array manager queries the selected arrays to discover which of their devices are replicated. Detailed information about the selected arrays and the number of replicated devices they support appears in the **Replicated Array Pairs** area of the Configure Array Managers window.

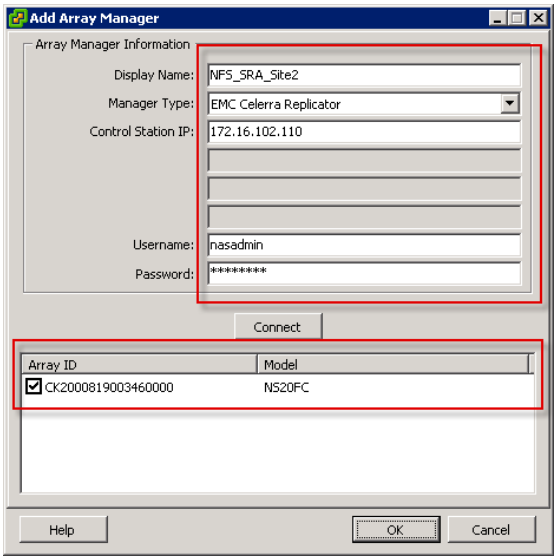
Figure 10: Enter array manager information for protected site



10. Click **Next** to configure array managers at the recovery site.
11. On the **Recovery Site Array Managers** page of the Configure Array Managers wizard, click Add.

    The procedure for configuring these arrays is identical to the procedure for configuring the arrays at the protected site, described in steps Step 5 through Step 8.

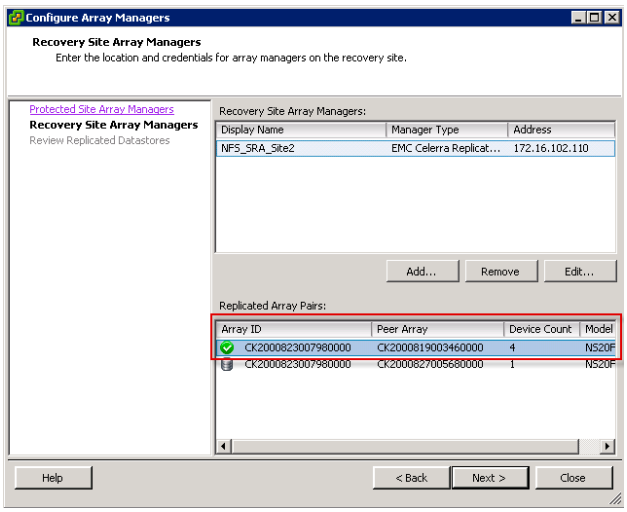
Figure 11: Enter array manager information for recovery site



12. Click **OK.**

    The array manager at the recovery site queries the selected arrays to discover which of their devices are replicated, and displays detailed information about the selected arrays and the number of replicated devices they support in the **Replicated Array Pairs** area of the Configure Array Managers window. A green checkmark icon distinguishes arrays that have peers at the protected site.

Figure 12: Replicated array pairs shown in Configure Array Managers window

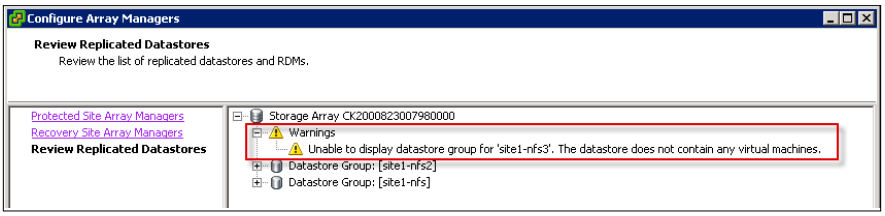


13. Click **Next** to display the list of replicated datastore groups.

    On the **Review Replicated Datastores** page, you can expand each datastore group to see which datastores it contains and the devices that it uses. If the list of datastore groups is not what you expected, you need to correct it before continuing.

    NOTE: Only those datastores used by at least one virtual machine are displayed. You can add the virtual machine after configuring the array manager. When you add the first virtual machine, Site Recovery Manager will re-compute the datastore groups. For this example, **VM site1-vm5** was added to the NFS store.

Figure 13: Warning shown for datastores that do not contain any virtual machines


Configure Array Managers
Review Replicated Datastores
Review the list of replicated datastores and RDMs.
Protected Site Array Managers
Recovery Site Array Managers
Review Replicated Datastores
Storage Array CK2000823007980000
Warnings
Unable to display datastore group for 'site1-nfs3'. The datastore does not contain any virtual machines.
Datastore Group: [site1-nfs2]
Datastore Group: [site1-nfs]

14. Click **Finish** to complete the configuration of the array managers.

Step 3: Set up inventory mapping

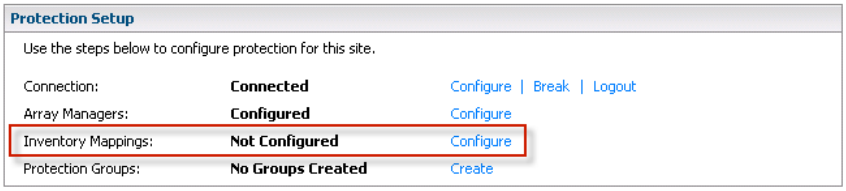
Inventory mappings establish recovery site defaults for the virtual machine folders, networks, and resource pools to which recovered virtual machines are assigned. You create these mappings at the protected site, and they apply to all virtual machines in all protection groups at that site.

Inventory mappings are optional, but recommended. They provide a convenient way to specify how resources at the protected site are mapped to resources at the recovery site. These mappings are applied to all members of a protection group when the group is created, and can be reapplied as needed (for example, when new members are added). If you do not create them, you must specify mappings individually for each virtual machine that you add to a protection group. A virtual machine cannot be protected unless it has valid inventory mappings for networks, folders, and resource pools. You do not need to specify inventory mappings for resources that are not used by protected virtual machines.

Procedure

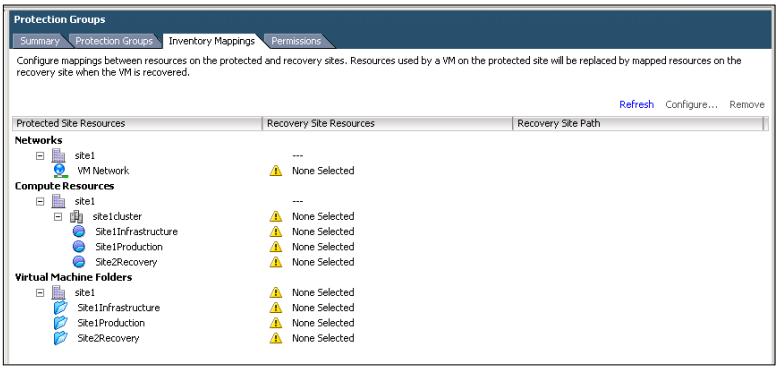
1. Open a vSphere Client and connect to the VMware vCenter server at the protected site. Log in as a vSphere administrator.
2. Click the **Site Recovery** icon on the vSphere Client Home page.
3. In the **Protection Setup** area of the **Summary** window, navigate to the **Inventory Mappings** line and click **Configure**.

Figure 14: Configure inventory mappings


Protection Setup
Use the steps below to configure protection for this site.
Connection: Connected Configure | Break | Logout
Array Managers: Configured Configure
Inventory Mappings: Not Configured Configure
Protection Groups: No Groups Created Create

The **Inventory Mappings** page displays a tree of resources at the protected site and a corresponding tree of resources at the recovery site. For any protected site resource that does not have an inventory mapping, the corresponding item in the recovery site tree is listed as **None Selected**.

Figure 15: Inventory Mapping interface before any mapping



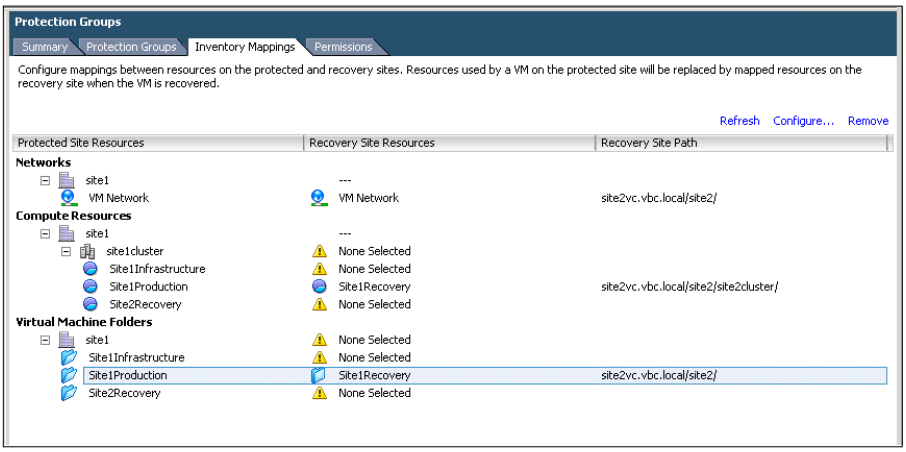
4. To configure mapping for a resource, right-click it in the **Protected Site Resources** column and click **Configure**.
5. Expand the top-level folder in the Configure Inventory Mapping window and navigate to the recovery site resource (network, resource pool, or folder) to which you want to map the protected site resource you selected in Step 4. Select the resource and click **OK**.

   The selected resource is displayed in the **Recovery Site Resources** column, and its path relative to the root of the recovery site vCenter is displayed in the **Recovery Site Path** column.

The following table summarizes the mapping that was created in this environment:

RESOURCE TYPE	PROTECTED SITE RESOURCE	RECOVERY SITE RESOURCE
Network	VM Network	VM Network
Resource Pool	Site1Production	Site1Recovery
Folder	Site1Production	Site1Recovery

Figure 16: Inventory Mapping interface after mappings



6. To undo an inventory mapping, right-click it and click **Remove**.

Step 4: Set up protection group

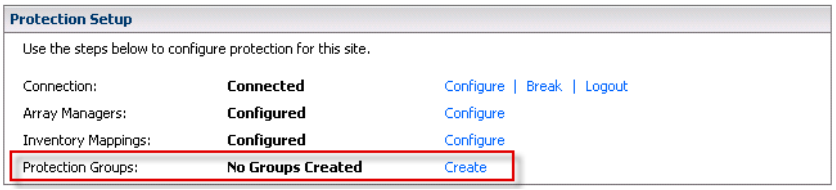
Site Recovery Manager organizes virtual machines into protection groups based on the datastore group that they use. All virtual machines in a protection group store their files within the same datastore group, and all failover together.

To create a protection group, you select a datastore group, and then specify a non-replicated datastore at the recovery site where Site Recovery Manager can create placeholders for members of the protection group. The placeholder datastore should be accessible to all hosts in the recovery cluster. It should not be replicated and can be relatively small.

Procedure

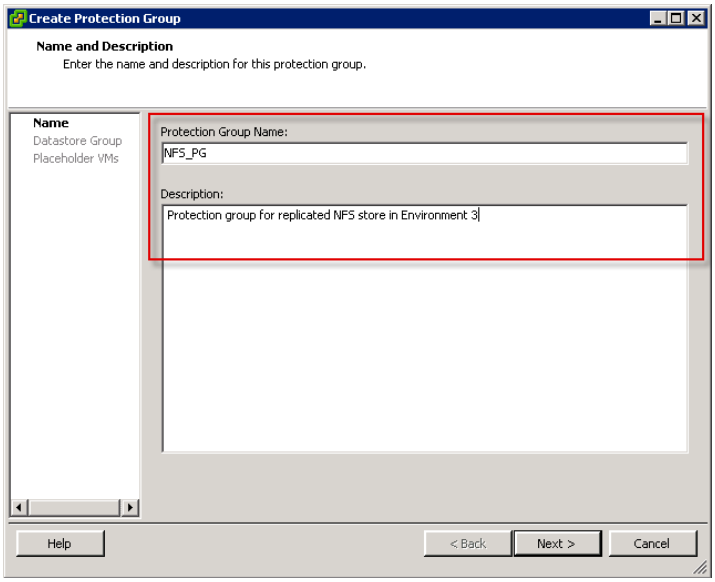
1. Open a VMware vSphere Client and connect to the VMware vCenter server at the protected site. Log in as a VMware vSphere administrator.
2. Click the **Site Recovery** icon on the VMware vSphere Client Home page.
3. In the **Protection Setup** area of the **Summary** window, navigate to the **Protection Groups** line and click **Create**.

Figure 17: Create protection group



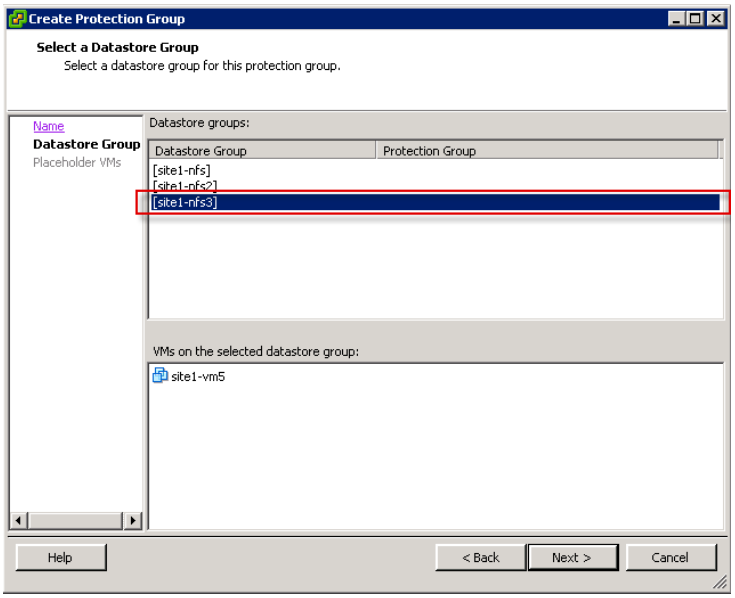
4. On the **Name and Description** page of the Create Protection Group wizard, type a name and optional description for the protection group, then click **Next**.

Figure 18: Enter protection group name and description



5. On the **Select a Datastore Group** page of the Create Protection Group wizard, select a datastore group from the list, then click **Next**.

Figure 19: Select a datastore group for the protection group being created



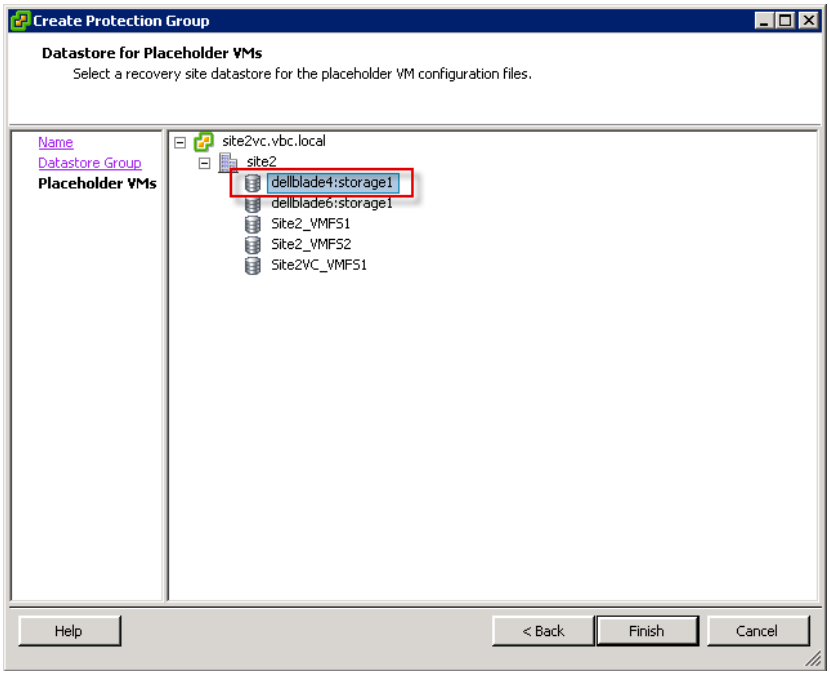
The datastore groups listed on this page are the ones that were discovered when you configured the array managers. Each datastore in the list is replicated to the recovery site, and supports at least one virtual machine at the protected site. When you select a datastore group, the virtual machines that it supports are listed in the **VMs on the selected datastore group** field, and are automatically included in the protection group.

6. On the **Datastore for Placeholder VMs** page of the Create Protection Group wizard, select a datastore group from the list.

   The datastores listed on this page exist only at the recovery site. The datastore that you select is used to hold the files that constitute the placeholder virtual machines. These files are not large, so any datastore that is accessible to the recovery site host and cluster can be an appropriate choice here.[9]

[9] The example here uses a replicated NFS store. You may have a different storage device type (e.g. iSCSI or FC). In this case, you may see all datastores are displayed including replicated datastores and temporary datastores used for test. Users must note not to use the replicated datastores and temporary datastores for holding the placeholder virtual machines.

Figure 20: Select datastore for placeholder virtual machines



7. Click **Finish** to create the protection group.

Site Recovery Manager creates a protection group that includes all of the virtual machines on the datastore you selected in Step 5. Placeholders are created and inventory mappings are applied for each member of the group. If any group member cannot be mapped to a folder, network, and resource pool on the recovery site, it is listed with a status of **Mapping Missing**, and no placeholder can be created for it.

Step 5: Set up recovery plan

A recovery plan controls how virtual machines in a protection group are recovered. It is stored in the Site Recovery Manager database at the recovery site, and executed by the Site Recovery Manager server at the recovery site.

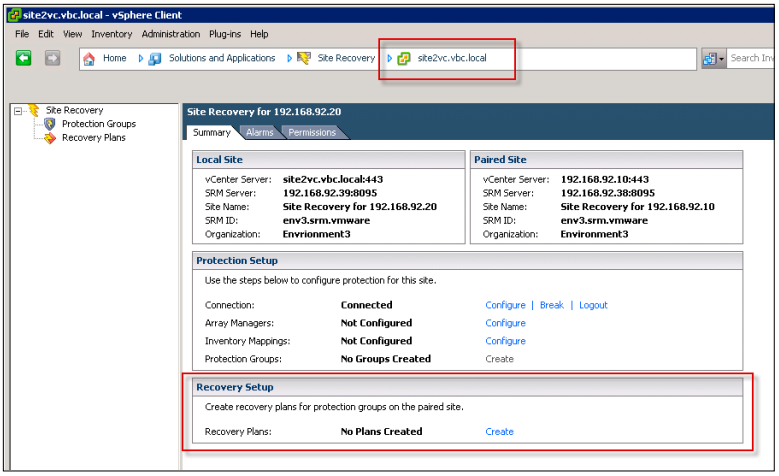
A simple recovery plan assigns all virtual machines in a protection group to two networks on the recovery site: a recovery network, and a test network. The recovery network is used in an actual recovery. The test network is a special network that is used only for testing the recovery plan, and does not typically allow the recovered virtual machines to communicate on your corporate network or the Internet. Site Recovery Manager can create a test network that exists only on one ESX Server for you, or you can create one yourself. Site Recovery Manager supports a recovery network that spans across the ESX Servers at the recovery site (i.e. vNetwork Distributed Switch (vDS)). In case your recovery plan calls for the need of vDS, you can create a vDS switch yourself for testing and failover recovery purposes.

A simple recovery plan includes a number of prescribed steps that use default values to control how protection group members are migrated to the protected site. You can customize a recovery plan to change default values, add steps to the plan itself and to the recovery of individual virtual machines, suspend non-critical virtual machines at the recovery site to make resources available for recovered machines, and so on.

Procedure

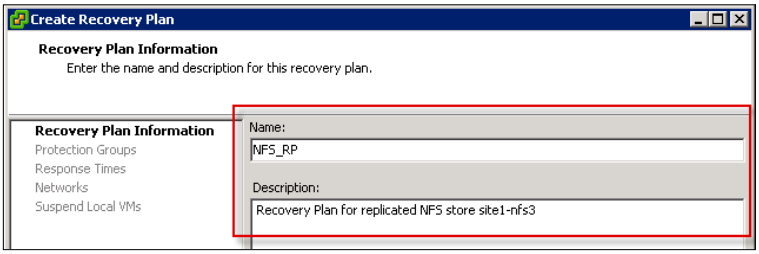
1. Open a vSphere Client and connect to the VMware vCenter server at the recovery site (e.g. site2vc.vbc.local). Log in as a vSphere administrator.
2. Click the **Site Recovery** icon on the vSphere Client Home page.
3. In the **Recovery Setup** area of the **Summary** window, navigate to the **Recovery Plans** line and click **Create**.[10]

Figure 21: Create recovery plan on recovery site



4. On the **Recovery Plan Information** page of the Create Recovery Plan wizard, type a name for the plan in the **Name** field and an optional description, then click **Next**.

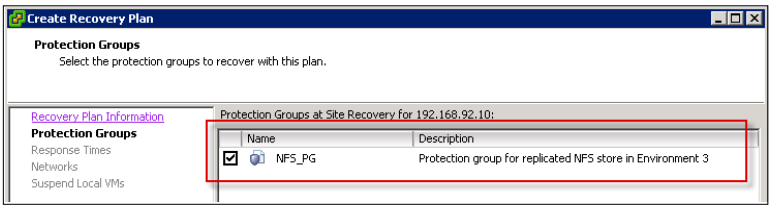
Figure 22 Enter recovery plan information



[10] On **Figure 21** you can see that Array Managers and Inventory Mappings are not configured on the recovery site since they have been configured on the protected site. Yet you still need to ensure that the SRAs are installed on the recovery site.

5. On the **Protection Groups** page of the Create Recovery Plan wizard, select one or more protection groups for the plan to recover, then click **Next**.

Figure 23: Select protection group for the recovery plan



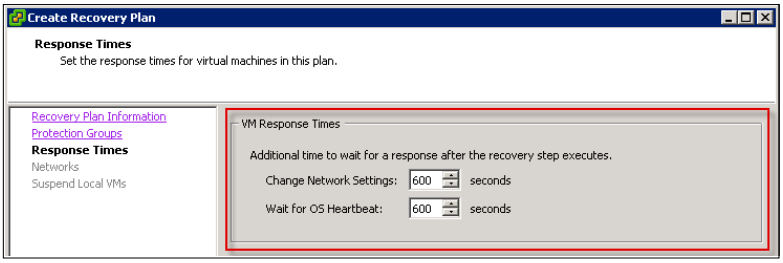
6. On the **Response Times** page of the Create Recovery Plan wizard, specify how long you want the recovery plan to wait for a response from a virtual machine after various recovery plan events, and then click **Next**.

There are two values that you can specify:

- Change Network Settings If the virtual machine does not acquire the expected IP address within the specified interval after a recovery step that changes network settings, an error is reported and the recovery plan proceeds to the next virtual machine.
- Wait for OS Heartbeat If the virtual machine does not report an OS heartbeat within the specified interval after being powered on, an error is reported and the recovery plan proceeds to the next virtual machine.

NOTE: Responses cannot be detected on virtual machines that do not have VMware Tools installed.

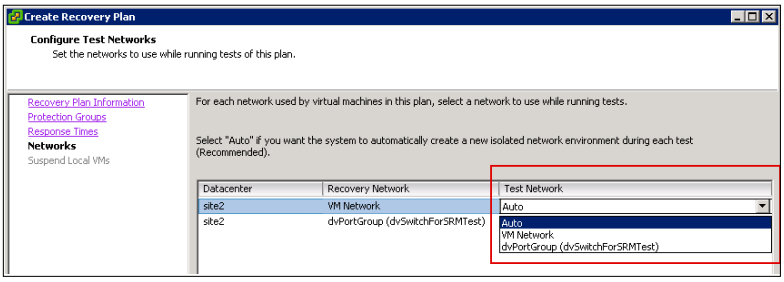
Figure 24: Configure virtual machine response times for the recovery



7. On the **Configure Test** Networks page of the Create Recovery Plan wizard, select a recovery site network to which recovered virtual machines connect to during recovery plan tests, and then click **Next**.

   By default, the test network is specified as **Auto**, which creates an isolated test network on one ESX Server for you. If you would prefer to specify an existing recovery site network as the test network (e.g. a vDS portgroup that spans across your recovery ESX Servers), click **Auto** and select the network from the drop-down control.

Figure 25: Configure test network for recovery plan



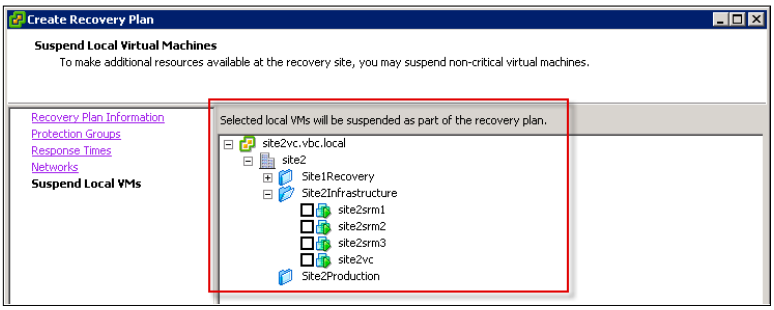
8. On the **Suspend Local Virtual Machines** page of the Create Recovery Plan wizard, select any virtual machines at the recovery site that the recovery plan should suspend.

   Suspending local virtual machines frees resources for use by recovered virtual machines. The virtual machines that you specify here are suspended during a test recovery as well as during an actual recovery.

   You can choose to suspend no virtual machines if doing so fits your requirements.'

   After a test recovery, the suspended virtual machines are powered on again.

Figure 26 Select non-critical local virtual machines to be suspended during recovery



9. Click **Finish** to create the recovery plan.

Step 6: Customize IP properties

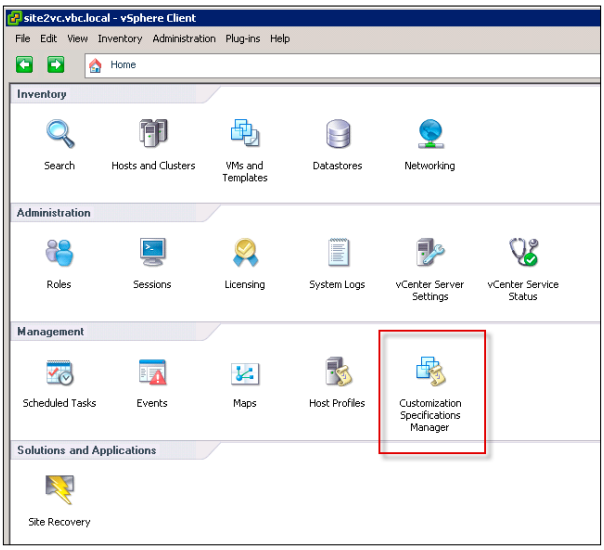
To customize the network properties of a virtual machine, customers can invoke the **Customization Specification Manager** on the recovery site to create a new customization specification and associate it with the corresponding virtual machine. Note that Site Recovery Manager only allows IP adapter properties to be updated through this mechanism. Other virtual machine properties such as registration information, time zone and administrator password are inherited from vCenter regardless of the input in the wizard.

Site Recovery Manager also provides **a batch IP customization tool** dr-ip-customizer.exe. Refer to the whitepaper titled "Automating Network Setting Changes and DNS Updates on Recovery Site Using VMware vCenter Site Recovery Manager" at http://viops.vmware.com/home/docs/DOC-1491 for more information.

To create a customization specification on recovery site:

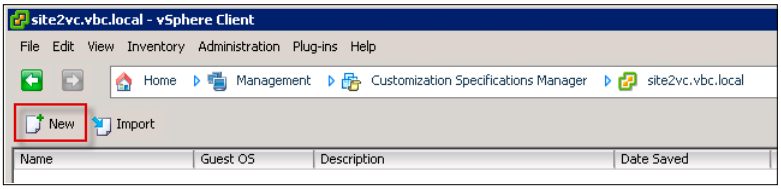
1. Open a vSphere Client and connect to the vCenter server at the protected site. Log in as a vSphere administrator.
2. Click the **Customization Specification** icon on the vSphere Client Home page.

Figure 27: Customization Specification



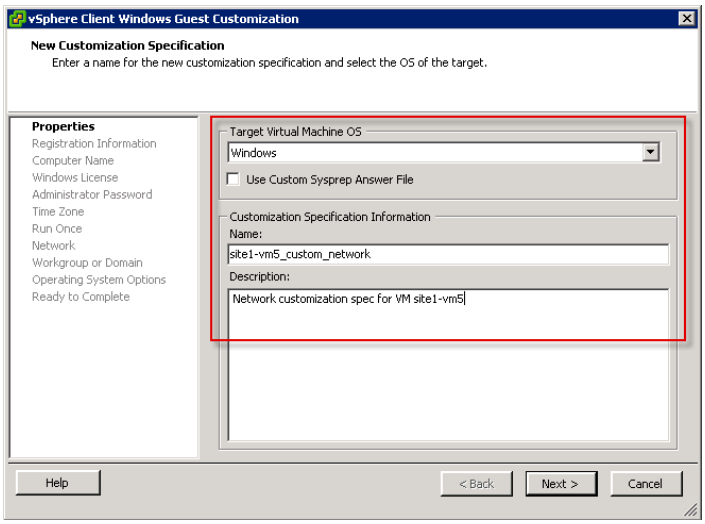
3. Select **New**.

Figure 28: Create new customization specification



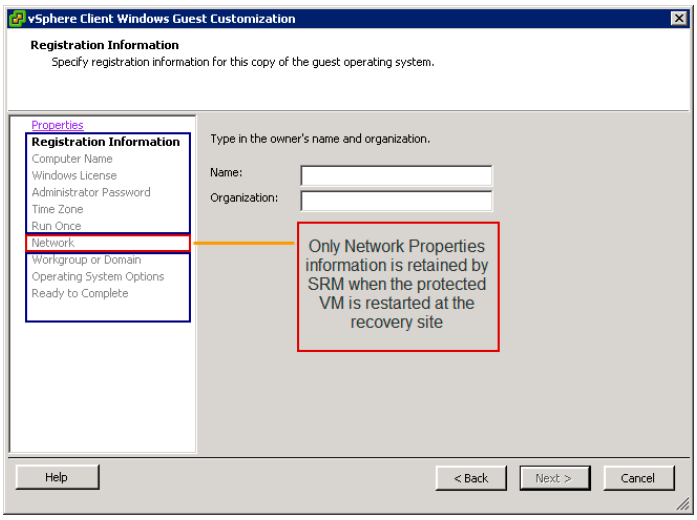
4. Enter name for Customization Specification (e.g. site1-vm5_custom_network).

Figure 29: Enter customization specification information



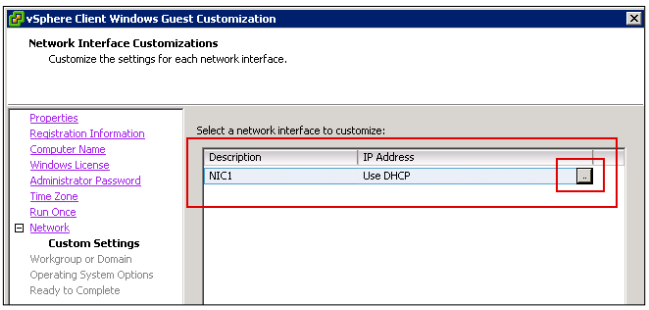
5. Click **Next**.
6. Follow Customization Specification Wizard through the steps until the **Network** page. Note the values entered before the Network page are ignored.

Figure 30: Enter network properties



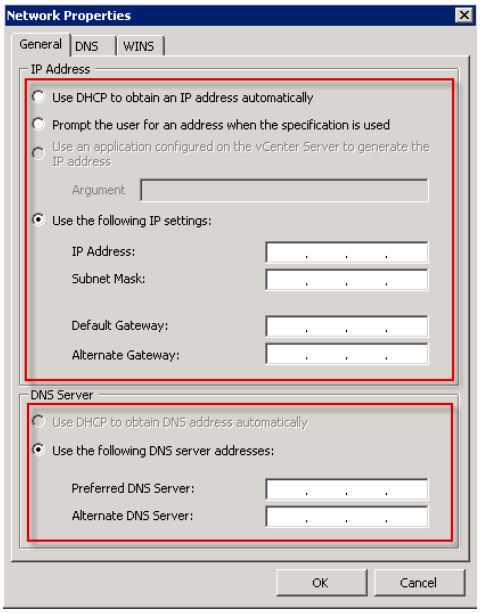
7. Select **Custom settings** and click **Next**.
8. Select a network interface to customize and click the button to the right of the selection.

Figure 31: Enter network custom settings



9. Configure the IP Address and the DNS Server according to your network environment.

Figure 32: Enter IP address and DNS server configurations

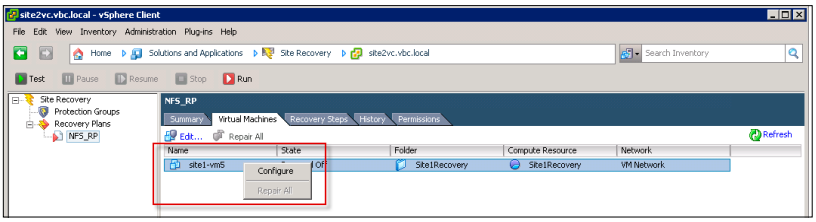


10. Follow the Customization Wizard until **Finish**.

To associate a virtual machine with the newly created customization specification:

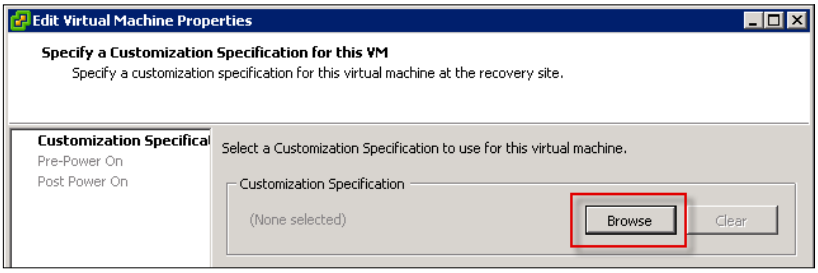
1. In Site Recovery, select the recovery plan that contains the virtual machine to be configured.
2. Go to Virtual Machines Tab and select the virtual machine.
3. Right Click on the virtual machine in the list and select **Configure**.

Figure 33: Configure selected virtual machine



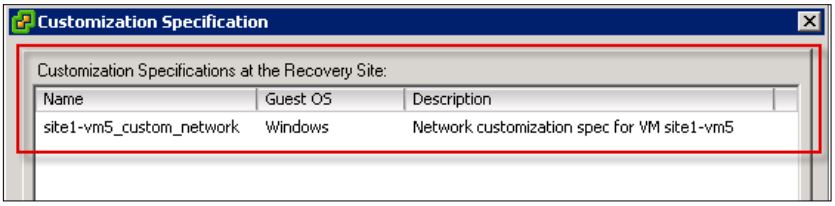
4. Click **Browse** to select the Customization Specification that you want to associate with this virtual machine.

Figure 34 Specify a customization specification for selected virtual machine


Edit Virtual Machine Properties
Specify a Customization Specification for this VM
Specify a customization specification for this virtual machine at the recovery site.
Customization Specifica
Pre-Power On
Post Power On
Select a Customization Specification to use for this virtual machine.
Customization Specification
(None selected)
Browse
Clear

5. Select the Customization Specification desired.

Figure 35: Select customization specification



6. Follow the wizard until **Finish**.

Step 7: Run test recovery

Site Recovery Manager enables you to '**Test**' a recovery plan by simulating a failover of virtual machines from the protected site to the recovery site. The benefit of using Site Recovery Manager to run a failover simulation against a recovery plan is that it allows you to confirm that the recovery plan has been setup correctly for the protected virtual machines. You will be able to confirm that the protected virtual machines startup in the correct order, taking into account the various application service dependencies for the protected virtual machines in your environment.

When you select the option to '**Test**' a recovery plan via Site Recovery Manager, the simulated failover is executed in an isolated environment that includes network and storage infrastructure at the recovery

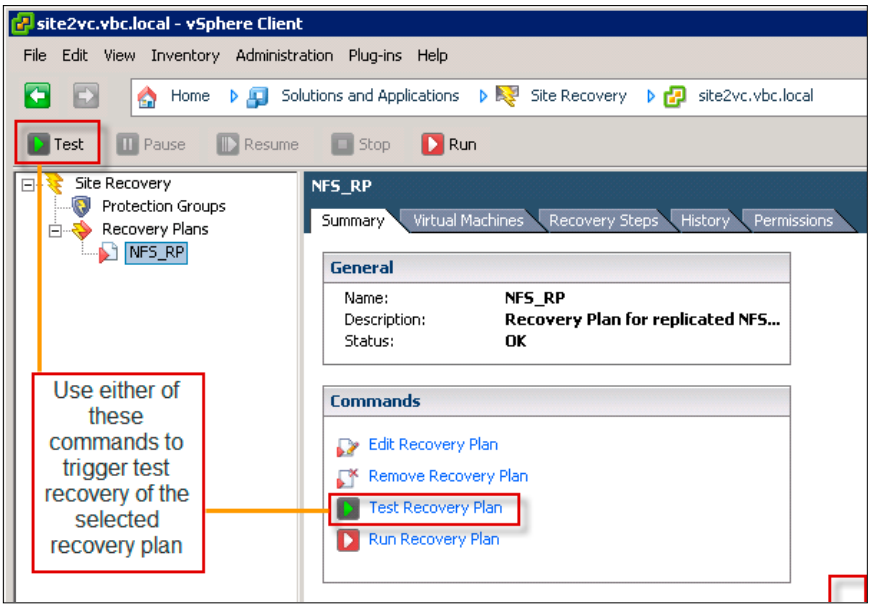
site that is isolated from the protected site (production environment) which ensures the protected virtual machines at the protected site are not subject to any kind of service interruption during the testing of the recovery plan. Site Recovery Manager will also create a test report that can be used to demonstrate your level of preparedness to the business or individual business units whose services are being protected by Site Recovery Manager as well as to the auditors and compliance officers if required.

The simulated failover completes by resetting the environment to be ready for the next event that could be another simulated failover, or an actual failover for a scheduled BC/DR test or in response to an event that resulted in the business declaring a disaster.

Procedure

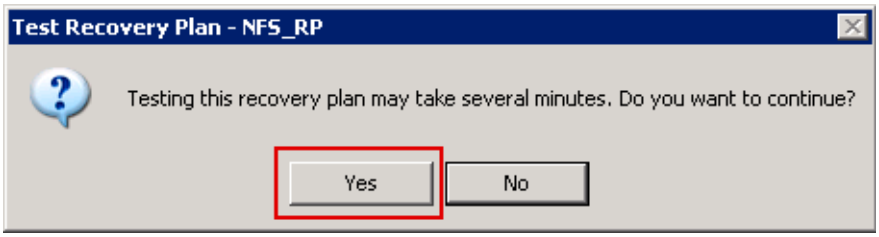
1. Open a vSphere Client and connect to the vCenter server at the recovery site. Log in as a user who has permission to test a recovery plan.
2. Click the **Site Recovery** icon on the vSphere Client Home page.
3. In the Site Recovery tree view, expand the Recovery Plans icon and click the recovery plan that you want to test.
4. In the Commands area of the Summary window, click Test Recovery Plan.

Figure 36: Trigger test recovery



When you see the confirmation prompt, click **Yes** to proceed with the test.

Figure 37: Confirmation prompt for test recovery



5. Click the **Recovery Steps** tab to monitor the progress of the test and respond to messages.

Figure 38: Create NAS Datastore During Test Recovery

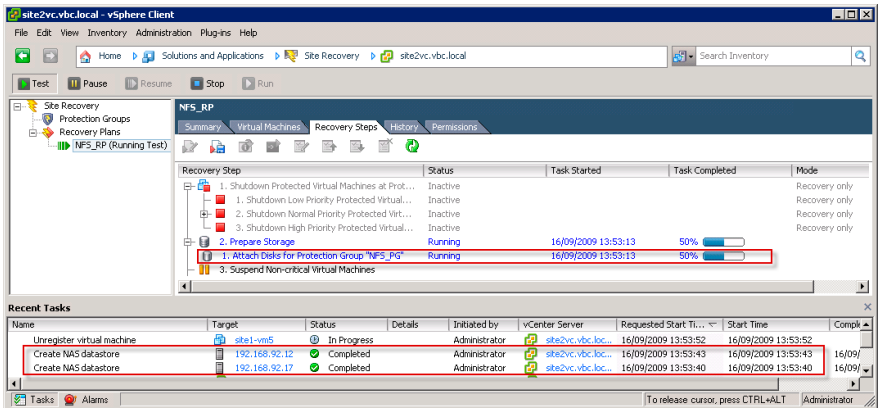


Figure 39: View of Datastores before Test Recovery – No NAS Store Yet

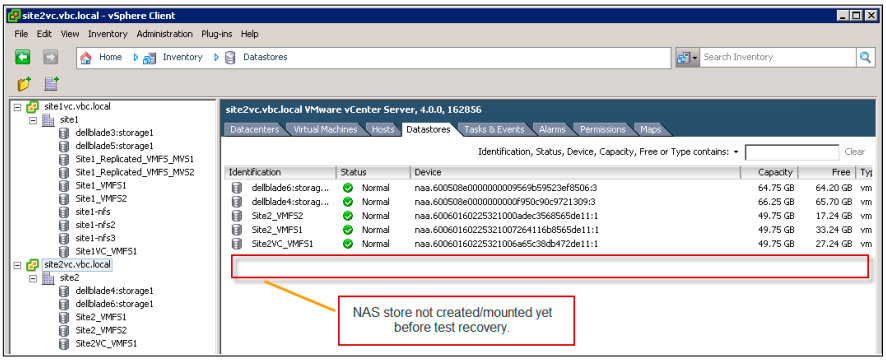
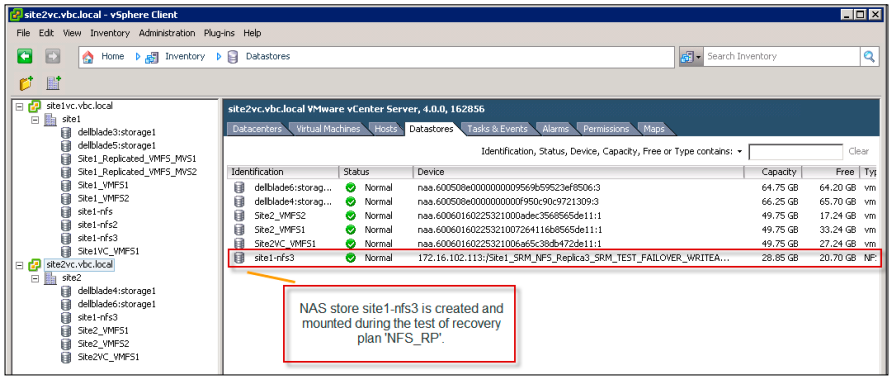


Figure 40: View of Datastores During Test Recovery – NAS store created and mounted

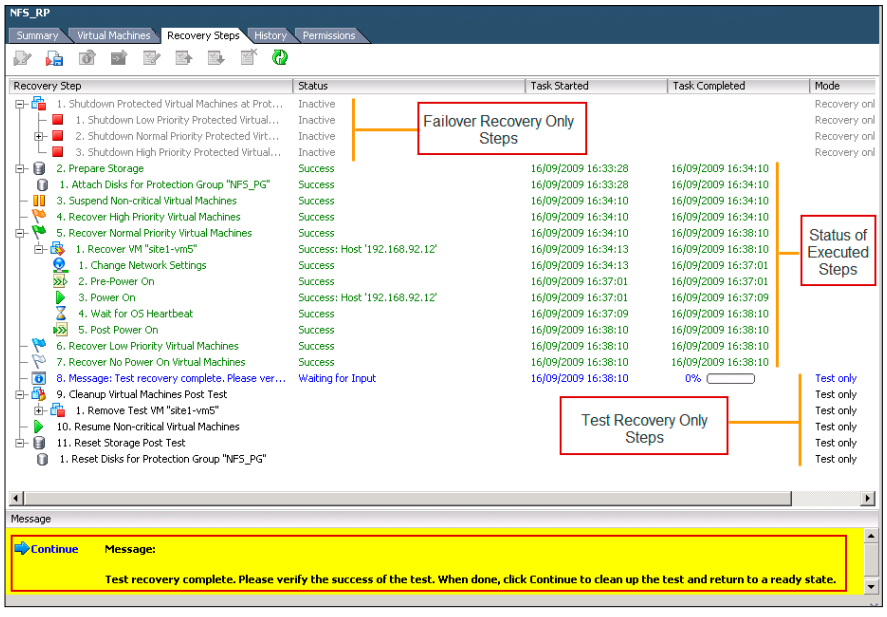

site2vc.vbc.local - vSphere Client
site2vc.vbc.local VMware vCenter Server, 4.0.0, 162856
NAS store site1-nfs3 is created and mounted during the test of recovery plan 'NFS_RP'.

For replicated NFS stores, Site Recovery Manager mounts a NAS datastore on recovery site during test recovery. See Figure 39 and Figure 40.

Unlike with FC and iSCSI stores, there is no **rescan HBA's** when working with NFS stores during test recovery.

While the simulated failover test is running, the status of each step that makes up the recovery plan can be monitored by going to Recovery Steps tab in the vSphere Client which will inform you what steps are currently running as well as what steps were completed. There are some steps in a recovery plan that will only be executed during a simulated test. 'Test Only' identifies these steps under the Mode column. There are also some steps that will only be executed during an actual failover. These steps are identified by 'Recovery only' under the Mode column.

Figure 41: Test recovery step run-down

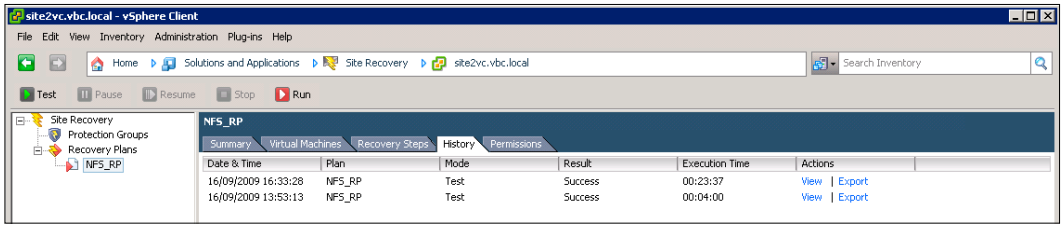

NFS_RP
Failover Recovery Only Steps
Status of Executed Steps
Test Recovery Only Steps
Continue
Message:
Test recovery complete. Please verify the success of the test. When done, click Continue to clean up the test and return to a ready state.

6. When the test recovery has finished powering on all of the protected virtual machines, it displays a message and requires confirmation before it can continue. Click **Continue** when you are ready for Site Recovery Manager to clean up and finish the test.

   Site Recovery Manager powers down and unregisters the test virtual machines, and then registers the placeholders back.

Site Recovery Manager provides an audit trail via a report that is generated automatically at the end of each Site Recovery Manager Test or Site Recovery Manager Recovery. The reports are accessible via the History tab and can be viewed by clicking on the View link under the Actions column, which will result in a browser window opening that contains a log of the steps executed during the test, with the total time to execute the recovery plan and the time it took to execute each step in the recovery plan.

Figure 42 Site Recovery Manager history tab – audit trail


site2vc.vbc.local - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Solutions and Applications Site Recovery site2vc.vbc.local
Search Inventory
Test Pause Resume Stop Run
Site Recovery
Protection Groups
Recovery Plans
NFS_RP
NFS_RP
Summary Virtual Machines Recovery Steps History Permissions
Date & Time Plan Mode Result Execution Time Actions
16/09/2009 16:33:28 NFS_RP Test Success 00:23:37 View | Export
16/09/2009 13:53:13 NFS_RP Test Success 00:04:00 View | Export

2. Site Recovery Manager Alarms and Site Status Monitoring

Awareness of the Site Recovery Manager alarms is an important part of understanding how Site Recovery Manager works across the protected and recovery sites. During the Site Recovery Manager product evaluation it is recommended that, where possible and without impact to your production environment, failures or conditions be created in the protected and recovery site that will result in the generation of Site Recovery Manager alarms. The generation of these Site Recovery Manager alarms will serve as validation that Site Recovery Manager is monitoring both the protected and recovery site correctly.

Each Site Recovery Manager server monitors the CPU utilization, disk space, and memory consumption of the guest on which it is running, and also maintains a heartbeat with its peer Site Recovery Manager server. vCenter events are sent if any of these measures falls outside of configured bounds.

Site Recovery Manager supports the configuration of event-triggered alarms so that you can associate a notification action with any given Site Recovery Manager Alarm Event. These alarms are configured via the Site Recovery Manager UI.

Site Recovery Manager supports the following alarm notification actions:

- **Send a notification e-mail** to a specific email address
- **Send a notification trap** to vCenter trap receivers
- **Run a script** on vCenter Server

Please refer to Chapter 5 – Customizing Site Recovery Manager in the Administrators Guide for Site Recovery Manager that details how to setup the alarm actions listed above.

Failure of either site generates events that can be associated with VMware vCenter alarms.

- Problems with the local site (e.g. resource constraints)

Problems with remote site (e.g. unable to ping remote site which may indicate a disaster)

- Remote site failure is reflected in the Site Recovery Manager Alarm Events and will not automatically trigger a recovery. This must be initiated manually.

Site Recovery Manager raises VMware vCenter events for the following conditions:

- Disk Space Low.
- CPU use exceeded limit.
- Memory low.

- Remote Site not responding.
- Remote Site heartbeat failed.
- Recovery Plan Test started, ended, succeeded, failed, or cancelled.
- Virtual Machine Recovery started, ended, succeeded, failed, or reports a warning.

As a starting point during the Site Recovery Manager Evaluation it is recommended that you complete the Action setup for the Site Recovery Manager Alarm Events listed below for the protected and recovery sites. You should be able to trigger these events in your environment without impacting your production environment, with the goal being that you see first-hand how Site Recovery Manager responds and notifies you when subjected to one of the failure events listed below.

- Remote Site Down.
- Remote Site Ping Failed.
- Replication Group Removed.
- Recovery Plan Destroyed.
- License Server Unreachable.

As you become more familiar with Site Recovery Manager, its associated workflows that allow you to **Test** your recovery plans as well as **Run** your recovery plan which results in the failover of services from your protected site to your recovery site, it is recommended that you work through the list of **Site Recovery Manager Alarm Events**. These can be accessed via the **Alarms** tab, as depicted in Figure 43 and enable the appropriate notification **Actions** for any additional Site Recovery Manager Alarm Events that you deem to be important for your environment.

2.1. Exercise: Configure Site Recovery Manager Alarms

SRM Alarms	**Configure action for a SRM Alarm**	Configure action for alarm 'Remote Site Down' 1. Configure alarm action to send out notification email.	10 minutes

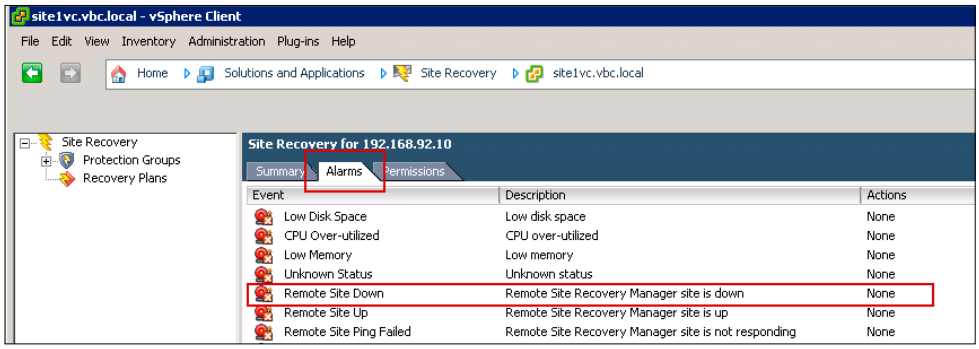
Step 1: Configure alarm action to send out notification email

Procedure

1. Open a vSphere Client and connect to the vCenter server at the recovery site. Log in as a vSphere administrator.
2. Click the **Site Recovery** icon on the vSphere Client Home page.

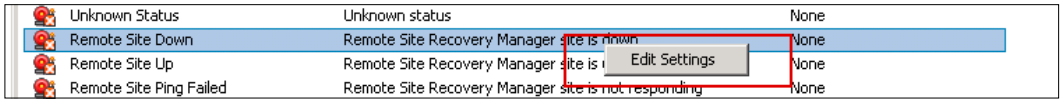
3. In the main window, click the **Alarms** tab to display the list of Site Recovery Manager alarms.

Figure 43: Site Recovery Manager alarms tab


site1vc.vbc.local - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Solutions and Applications Site Recovery site1vc.vbc.local
Site Recovery
Protection Groups
Recovery Plans
Site Recovery for 192.168.92.10
Summary Alarms Permissions
Event Description Actions
Low Disk Space Low disk space None
CPU Over-utilized CPU over-utilized None
Low Memory Low memory None
Unknown Status Unknown status None
Remote Site Down Remote Site Recovery Manager site is down None
Remote Site Up Remote Site Recovery Manager site is up None
Remote Site Ping Failed Remote Site Recovery Manager site is not responding None

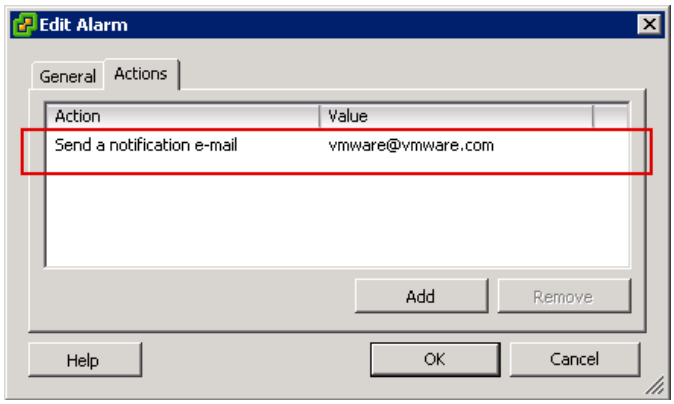
4. Right-click on **Remote Site Down** and click **Edit Settings**.

Figure 44 Edit settings for alarm 'Remote Site Down'


Unknown Status Unknown status None
Remote Site Down None
Remote Site Up None
Remote Site Ping Failed None
Edit Settings

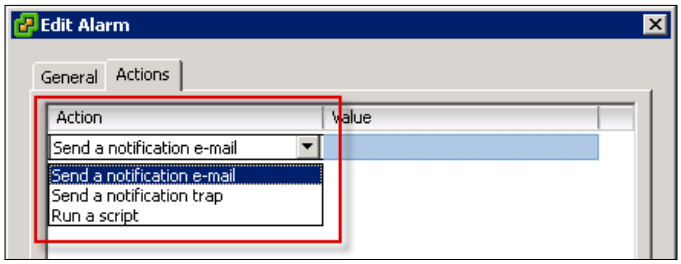
5. In the Edit Settings dialog box, click the Actions tab. In the Actions window, click **Add** to add an action.

Figure 45: Add action for alarm 'Remote Site Down'



Use the default action **Send a notification e-mail** and type in an email address in the Value column. (To change this action, click it and select a different action from the drop-down box.)

Figure 46 Select action for alarm 'Remote Site Down'

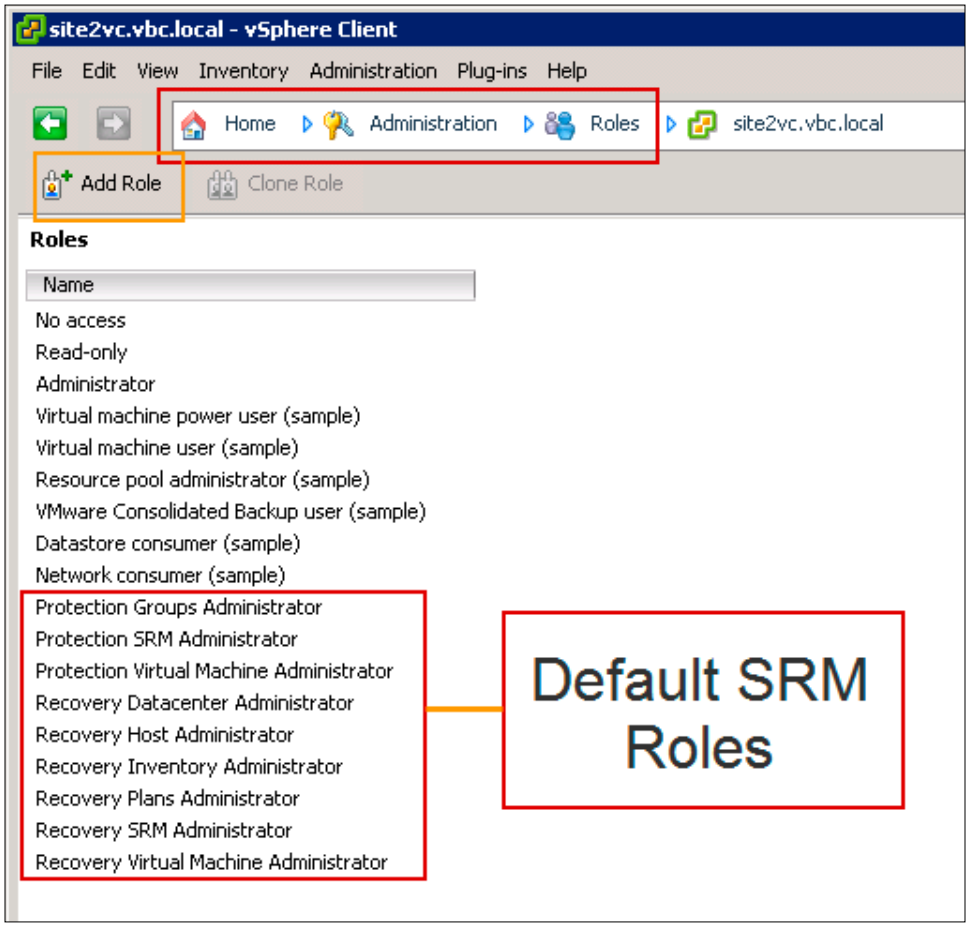


3. Site Recovery Manager Roles and Privileges

This section provides an overview of the Site Recovery Manager roles and the types of Site Recovery Manager privileges that can be set. Authorization in Site Recovery Manager uses the same authorization model as vCenter Server.

Figure 47 show the default Site Recovery Manager roles that become available for use after the Site Recovery Manager plug-in has been installed and enabled for use. To access these roles click on the **Administration** icon in the toolbar and click on the **Roles** tab to see a list of all the roles that are available. These default Site Recovery Manager roles provide the ability to delegate control to a very granular level.

Figure 47: Default Site Recovery Manager Roles



There are two sets of roles. The first set contains the roles required for the primary site user to administer protection and the Site Recovery Manager roles are prefixed by **Protection**. The second set contains the roles required for the secondary site user to administer recovery and the Site Recovery Manager roles are prefixed by **Recovery.**

Protection Side Site Recovery Manager Roles

Protection Virtual Machine Administrator: This role should be assigned on the protected Virtual Machine object in the VC inventory. It grants the associated user the ability to setup and modify the protection characteristics of the protected virtual machine.

Protection Site Recovery Manager Administrator: This role should be assigned on the Service Instance object in the primary Site Recovery Manager inventory. It grants the associated user the ability to pair two sites, configure inventory mappings, and SAN arrays.

Protection Groups Administrator: This role should be assigned on the Primary Configuration/Protection Service object in the Site Recovery Manager inventory. It grants the associated user the ability to create and modify protection profiles/groups.

Recovery Side Site Recovery Manager Roles

Recovery Inventory Administrator: This role should be assigned on the root of the VC inventory. It grants the associated user the ability to view customization specifications existing on the secondary site.

Recovery Datacenter Administrator: This role should be assigned on the Datacenter object in the VC inventory where the virtual machines will be recovered. It grants the associated user the ability to view available datastores and perform recovery (shadow) virtual machine customizations.

Recovery Host Administrator: This role should be assigned on the Host or DRS cluster object in the VC inventory where the virtual machine will be recovered. It grants the associated user the ability to configure virtual machine components during recovery.

Recovery Virtual Machine Administrator: This role should be assigned on the Folder and Resource Pool objects in the VC inventory where the recovery (shadow) virtual machines are to be placed. It grants the associated user the ability to create and add shadow virtual machines to the resource pool and the folder as well as the ability to reconfigure and customize the shadow virtual machines at runtime and during the process of recovery.

Recovery Site Recovery Manager Administrator: This role should be assigned on the Service Instance object in the secondary Site Recovery Manager inventory. It grants the associated user the ability to configure SAN arrays and create protection profiles.

Recovery Plans Administrator: This role should be assigned on the Secondary Configuration/Recovery Service object in the Site Recovery Manager inventory. It grants the associated user the ability to reconfigure protection and shadow virtual machines and setup and run recovery.

NOTE: VMware vCenter already defines a Read-Only system role, which can be used to grant users the ability to view the Site Recovery Manager service. In addition, the **Administrator** role can be used to grant user complete control over both the protection and recovery Site Recovery Manager components.

Site Recovery Manager also allows for the creation of custom Site Recovery Manager roles by allowing you to either add a role or to clone one of the default Site Recovery Manager roles, and then by editing the cloned Site Recovery Manager role, you can select which privileges should be associated to the custom Site Recovery Manager role that you are creating. Figure 50 shows a Custom Site Recovery Manager Role and all the privileges that can be selected to complete the creation of the Site Recovery Manager Custom Role.

3.1. Exercise: Create a Site Recovery Manager Custom Role

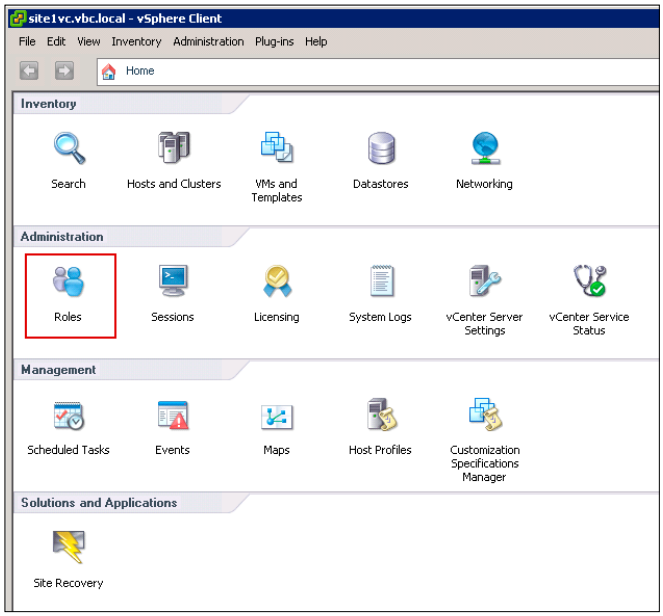
SRM Roles	**Custom Role Creation**	Create a SRM Custom Role 1. Create a SRM custom role with SRM specific privileges.	10 minutes

Step1: Create a Site Recovery Manager custom role with Site Recovery Manager specific privileges.

Procedure

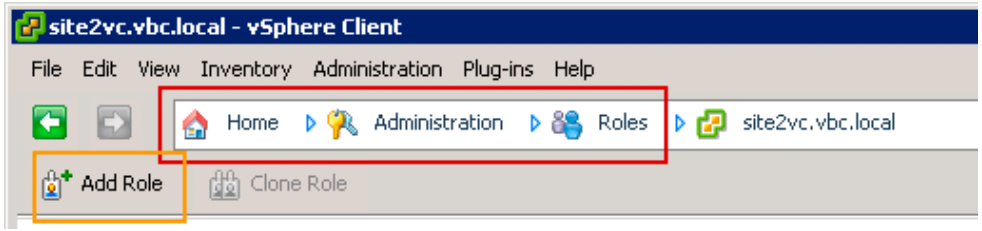
1. Open a vSphere Client and connect to the vCenter server at the protected site. Log in as a vSphere administrator.
2. Click the **Roles** icon on the vSphere Client Home page.

Figure 48: Administration of roles



3. Click on **Add Role**.

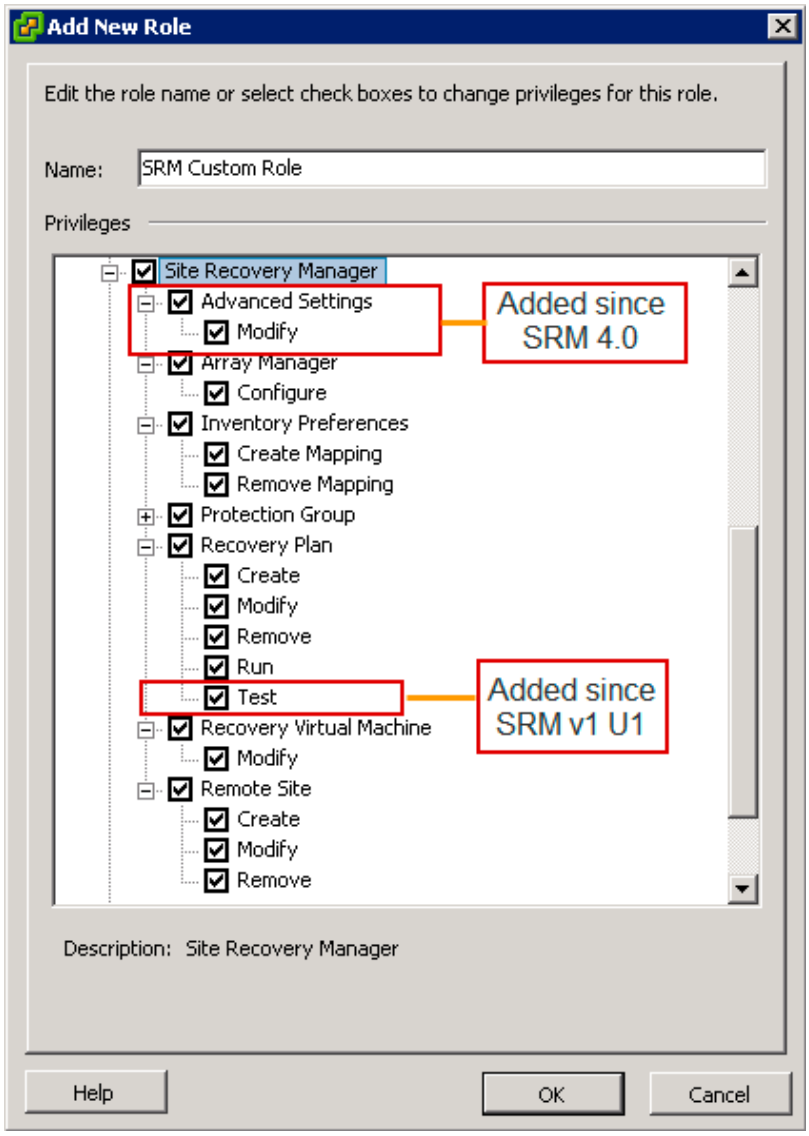
Figure 49: Add role



4. Input the name of the new role (e.g. Site Recovery Manager Custom Role) and select the privileges for the new role.

NOTE: In Site Recovery Manager 1.0 U1, a new privilege for running **test** recovery has been added and in Site Recovery Manager 4.0, a new privilege group **Advanced Settings** has been added. See Figure 50. You can find more details about Advanced Settings in Section 4.

Figure 50: Add Site Recovery Manager Custom Role



4. Site Recovery Manager Advanced Settings

In Site Recovery Manager 4.0, you can use the Advanced Settings dialog to view or change many custom settings for the Site Recovery Manager service.

The Advanced Settings dialog box provides an easy way for a user with adequate privileges to change a number of default values that affect the operation of various Site Recovery Manager features.

NOTE: Changes that you make in the Advanced Settings dialog boxes overwrite the contents of the Site Recovery Manager configuration file (vmware-dr.xml) on the Site Recovery Manager server host.

4.1. Optional Exercise: Change Advanced Settings

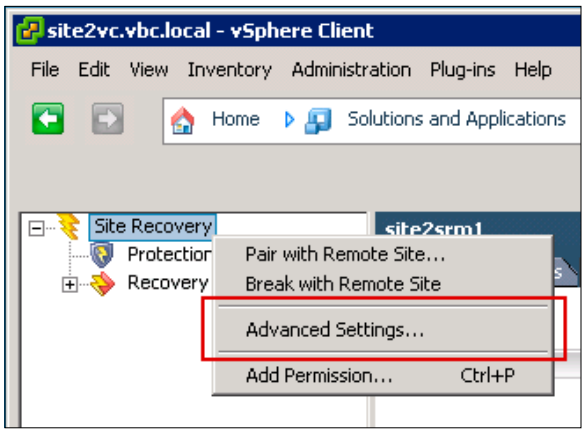
SRM Advanced Settings	**Change Advanced Settings**	Change Advanced Settings 1. Change one of the advanced settings, e.g. SanProvider. CommandTimeout	20 minutes

Step 1: Change one of the advanced settings

Procedure

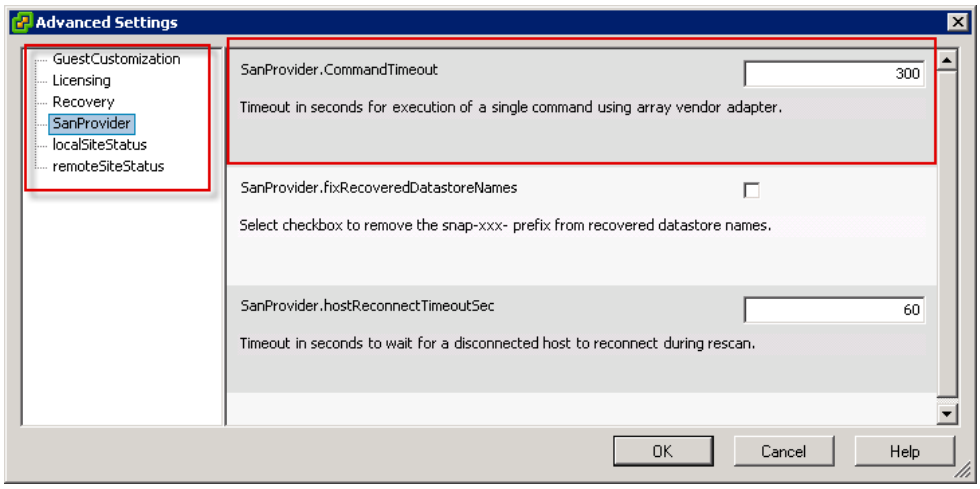
1. Open a vSphere Client and connect to the vCenter server at the recovery site. Log in as a vSphere administrator.
2. Click the **Site Recovery** icon on the vSphere Client Home page.
3. Right-click **Site Recovery** in the vSphere Client navigation pane and click **Advanced Settings**.

Figure 51: Configure Advanced Settings



4. In the navigation pane of the Advanced Settings window, click a setting category.

Figure 52: Change Advanced Settings



5. In the category window, make your changes.

   For example, you may want to change the SRA timeout that is represented by SanProvider.CommandTimeout in Figure 52.

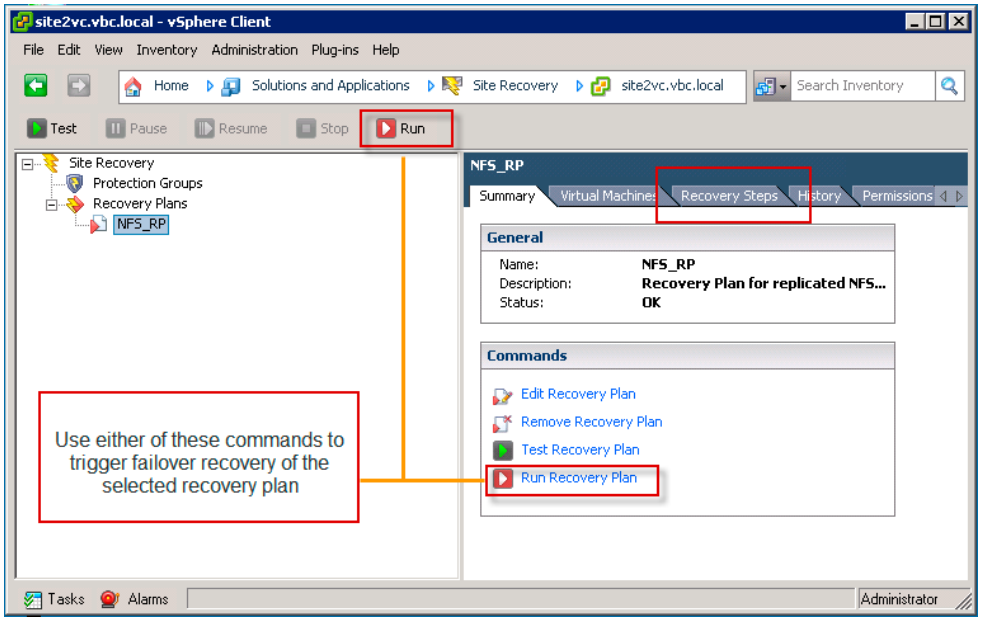
   a. Change SanProvider.CommandTimeout to 2 seconds

6. Click **OK** to save your changes and close the Advanced Settings window.
7. Now when you run Test Recovery, you will experience a failure.
8. Repeat steps 1-6 and change SanProvider.CommandTimeout back to 300 seconds.
9. Now when you run Test Recovery, you will experience a success.

5. Failover from Protected Site to Recovery Site

Site Recovery Manager enables you to '**Run**' a recovery plan that will result in the actual failover of virtual machines from the protected site. Similar to test recovery, failover operations are triggered via a button in the Site Recovery Manager UI on the recovery site. The failover process via Site Recovery Manager is rapid, repeatable, reliable, manageable and auditable.

Figure 53: Trigger failover



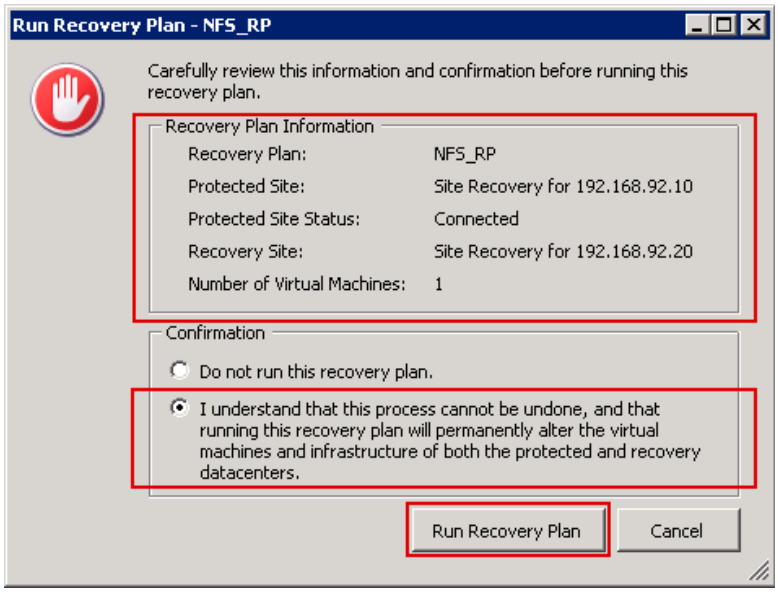
This example will show you how to work through an actual failover leveraging the Site Recovery Manager '**Run'** a recovery plan option.

In Figure 53, the Site Recovery Manager UI lists the recovery plan NFS_RP that was created in Section 1 There are two ways to initiate the actual failover, you can either click on the '**Run**' button or click on the '**Execute Recovery Plan'** link under the **Commands** section, and both are highlighted in Figure 53.

The **Run Recovery Plan** dialog box represented by Figure 54 warns you that you are about to run the a recovery plan which will result in changes to the protected virtual machines and the infrastructure of both the protected and recovery site datacenters. Click the **radio button** to confirm you understand the implications of running your recovery plan and then click on the **Run Recovery Plan** button that is highlighted in Figure 54 to start the failover of protected virtual machines from the protected site to the recovery site.

The **Run Recovery Plan** dialog box also provides a summary of the **Recovery Plan Information**. This includes the Recovery Plan that is going to be run, the names of the protected and recovery sites, the number of protected virtual machines that will be failed over, as well as a connectivity status from the recovery site back to the protected site.

Figure 54: Confirmation Dialog for Run Recovery Plan


Run Recovery Plan - NFS_RP
Carefully review this information and confirmation before running this recovery plan.
Recovery Plan Information
Recovery Plan: NFS_RP
Protected Site: Site Recovery for 192.168.92.10
Protected Site Status: Connected
Recovery Site: Site Recovery for 192.168.92.20
Number of Virtual Machines: 1
Confirmation
Do not run this recovery plan.
I understand that this process cannot be undone, and that running this recovery plan will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.
Run Recovery Plan
Cancel

While the failover is being executed, the status of each step that makes up the recovery plan can be monitored by going to **Recovery Steps** tab (highlighted in Figure 53) of the Site Recovery Manager UI on the recovery site. The UI informs you what steps are currently **Running** as well as what steps were completed. There are some steps in a recovery plan that will only be executed during a simulated test. 'Test Only' identifies these steps under the **Mode** column. There are also some steps that will only be executed during an actual failover. These steps are identified by **Recovery only** under the **Mode** column.

Once all the protected virtual machines have been failed over and reported to be powered on, you are ready to start validating that all application services restarted cleanly at the recovery site. In this case, the protected virtual machine **site1-vm5** from the NFS_PG is referred to. Once you have completed the validation of the failed over application services at the recovery site you are now in a position to report the successful failover to the business and allow the respective business users to access the application services, which are now being hosted on the recovery site.

NOTE: Site Recovery Manager will automatically perform a re-signature of the replicated iSCSI and FC datastores in the recovery site, which means **LVM.EnableResignature** will be set to **1** on the ESX hosts that have access to the replicated datastores in the recovery site. The re-signature that is initiated by Site Recovery Manager will result in the replicated datastores being presented with a prefix of **snap-xxx-**.

Site Recovery Manager automatically generates a report for each recovery plan execution. In this instance the report is for a Site Recovery Manager '**Run'** operation against the recovery plan that was selected. The report is accessible via the **History** tab and can be viewed by clicking on the **View** link under the **Actions** column. See Figure 42.

The steps to failback services from the recovery site back to the protected site once the disaster event is over are outlined in section 6.

The following is a recap of the high level tasks executed by Site Recovery Manager when performing a failover of virtual machines from the protected site to the recovery site via the '**Run**' a recovery plan option. Site Recovery Manager automates many of the tasks required at time of failover. With the push of one button, Site Recovery Manager:

- Powers down the protected virtual machines if there is connectivity between sites and they are online.
- Suspends data replication and Read/Write enable the replica datastores.

- Re-scans the ESX servers at the recovery site.
- Registers the replicated protected virtual machines.
- Suspends non-essential virtual machines at the recovery site if specified to free up resources for the protected virtual machines being failed over.
- Completes power-up of replicated protected virtual machines in accordance with the recovery plan.

6. Failback from Recovery Site to Protected Site

Failback in Site Recovery Manager 4.0 is the same process used in previous releases. As before the key to understanding failback is that very simply it is the same steps as failover but in the opposite direction.

In the previous section, a recovery plan was executed plan in 'Run' mode that essentially performed a live failover of the virtual machines. Once your virtual machines have been successfully recovered by Site Recovery Manager the next step will at some point in time be a failback.

The failback scenario covered as part of this evaluation will involve failing back to a site that is still in a good state after the DR event (i.e. the same equipment and configuration that was failed over from has remained.) If you suffer a total site loss of the site you failed over from then additional steps will obviously need to be followed before you can failback as you will need to recreate the environment at the lost site before commencing any failback.

To summarize the workflow:

1. Failover recovery plan from Site 1 (protected site) to Site 2 (recovery site)
2. Virtual machine named "site1-vm5" and its associated NFS export "site1-nfs3" successfully failed over to Site 2
3. Virtual machine "site1-vm5" now powered on and running successfully at Site 2

The goal is now to failback the NFS export containing Virtual machine "site1-vm5" to its original home at Site 1. In this example, you can see that NFS is used, but the same process applies for FC/iSCSI although at certain points storage rescans would be needed for those protocol types. These will be pointed out where appropriate.

The high-level steps for this failback will be:

1. Verify virtual machine failed over correctly.
2. Review state of storage at recovery site (Site 2) and failback site (Site 1).
3. Reverse storage replication so that replication now flows from Site 2 to Site 1 for the NFS export that this virtual machine resides in.
4. Configure Site Recovery Manager SRAs within Site 2 Site Recovery Manager server.
5. Configure Site Recovery Manager Inventory mapping within Site 2 Site Recovery Manager server.
6. Remove original protection group at Site 1 and recovery plan at Site 2 used for original virtual machine protection.
7. Remove from vCenter inventory virtual machine objects left behind at Site 1 for virtual machines that were failed over to Site 2.
8. Create protection group at Site 2 for datastore group containing this NFS export.
9. Create Recovery plan at Site 1 for this protection group created in step 8.
10. Test Recovery plan using Site Recovery Manager "Test" mode recovery plan functionality.
11. Failback using Site Recovery Manager "Run" mode recovery plan functionality.

Most of the steps for failback are essentially checks but it is worth running through this process thoroughly during this evaluation as not only will this process make any real failover / failback scenarios straightforward it also helps to increase understanding of the architecture and workflow of Site Recovery Manager.

You can now go through the steps in more detail.

1. **Verify virtual machine failed over correctly**. Before performing any failback, review the vCenter inventory at your recovery site to check everything is at it should be. In this example, the site 1 VMware vCenter instance is obviously still online at this time so it can be compared to the recovery site against the protected site in a single view if using Linked Mode vCenter.

Figure 55: Review vCenter Inventories

2. **Review state of storage at recovery site (Site 2) and failback site (Site 1)**. Before moving on, it is important to review the state of the storage at both sites to determine the storage point of view, and how it relates to the datastores or exports you are working with during the failback process. This example works from a single NFS export.

Figure 56: Review Site 1 storage

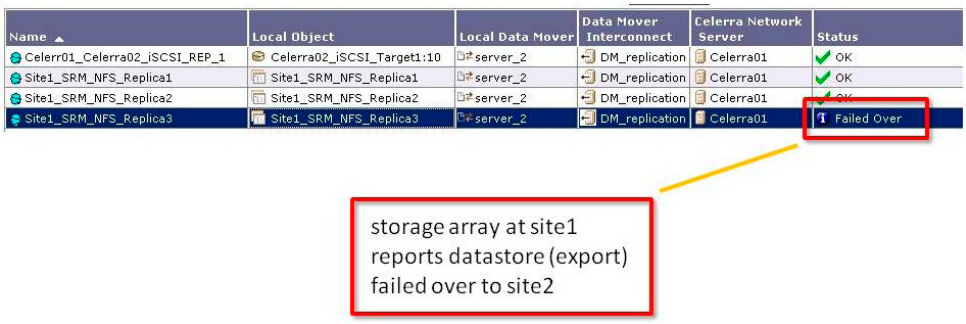


Figure 56 shows that the export/datastore that used to be presented at Site 1 has now been failed over successfully to the array at Site 2.

Figure 57: Review Site 2 storage

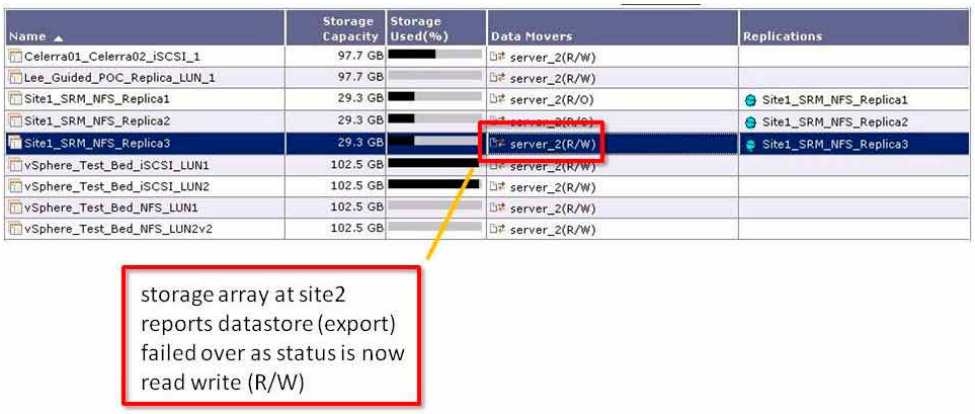
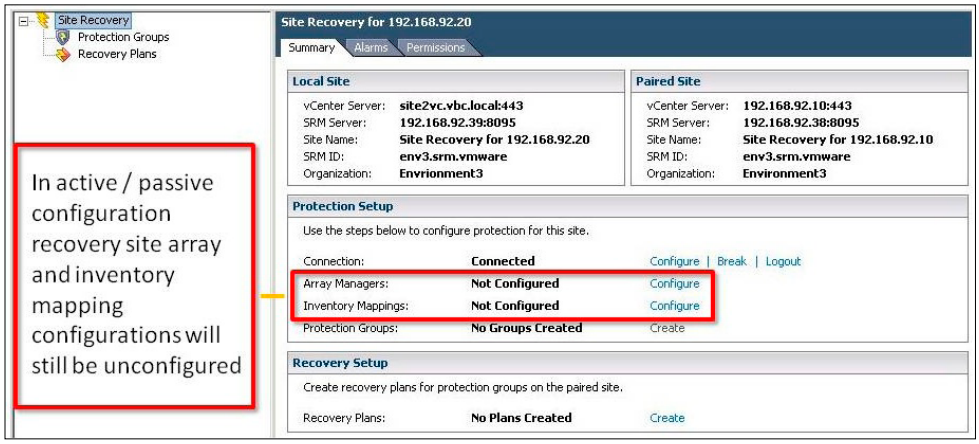


Figure 57 confirms that the export/datastore is now in read/write mode (R/W) on the Site 2 array. The export/datastore was placed into this mode during the Site Recovery Manager recovery plan being executed in '**Run**' mode to perform the failover.

3. **Reverse storage replication so that replication now flows from Site 2 to Site 1 for the NFS export the virtual machine resides in**. Before failback can be discussed from Site 2 to Site 1, the storage array replication needs to be reconfigured to replicate in that direction. Depending on the storage array replication technology being used your array may do this automatically if the Site 1 array is still available and responding (known as a dynamic swap). In most cases you will need to work with your storage teams to reverse the storage replication.
4. **Configure Site Recovery Manager SRAs within Site 2 Site Recovery Manager server**. A typical Site Recovery Manager configuration will be an active / passive configuration which basically means in the original state Site 1 will be the protected site and Site 2 will be the recovery site. This was the case for this example. In this kind of deployment there is no need -during the initial setup to configure the array managers or the inventory mappings within the Site Recovery Manager server at Site 2 until a failback operation is to be performed. This will typically look like Figure 58.

Figure 58: Site 2 configuration for failback


Site Recovery
Protection Groups
Recovery Plans
In active / passive configuration recovery site array and inventory mapping configurations will still be unconfigured
Site Recovery for 192.168.92.20
Summary
Alarms
Permissions
Local Site
vCenter Server: site2vc.vbc.local:443
SRM Server: 192.168.92.39:8095
Site Name: Site Recovery for 192.168.92.20
SRM ID: env3.srm.vmware
Organization: Envrionment3
Paired Site
vCenter Server: 192.168.92.10:443
SRM Server: 192.168.92.38:8095
Site Name: Site Recovery for 192.168.92.10
SRM ID: env3.srm.vmware
Organization: Environment3
Protection Setup
Use the steps below to configure protection for this site.
Connection: Connected Configure | Break | Logout
Array Managers: Not Configured Configure
Inventory Mappings: Not Configured Configure
Protection Groups: No Groups Created Create
Recovery Setup
Create recovery plans for protection groups on the paired site.
Recovery Plans: No Plans Created Create

NOTE: If your deployment is active/active which commonly means that from the outset both sites were defined as protected with each acting as the others recovery site then to have built that configuration your array managers and inventory mappings will already be configured at Site 2. If this applies to you skip to the next step.

Configuring the Array Managers (SRA's) at Site 2 is the same process used to configure the SRA's originally the only difference being that the array objects are now entered in a different order.

Figure 59 illustrates configuring the protected site array at Site 2. The array credentials entered here relate to the storage array that resides in Site 2.

Figure 59: Site 2 protected site array configuration

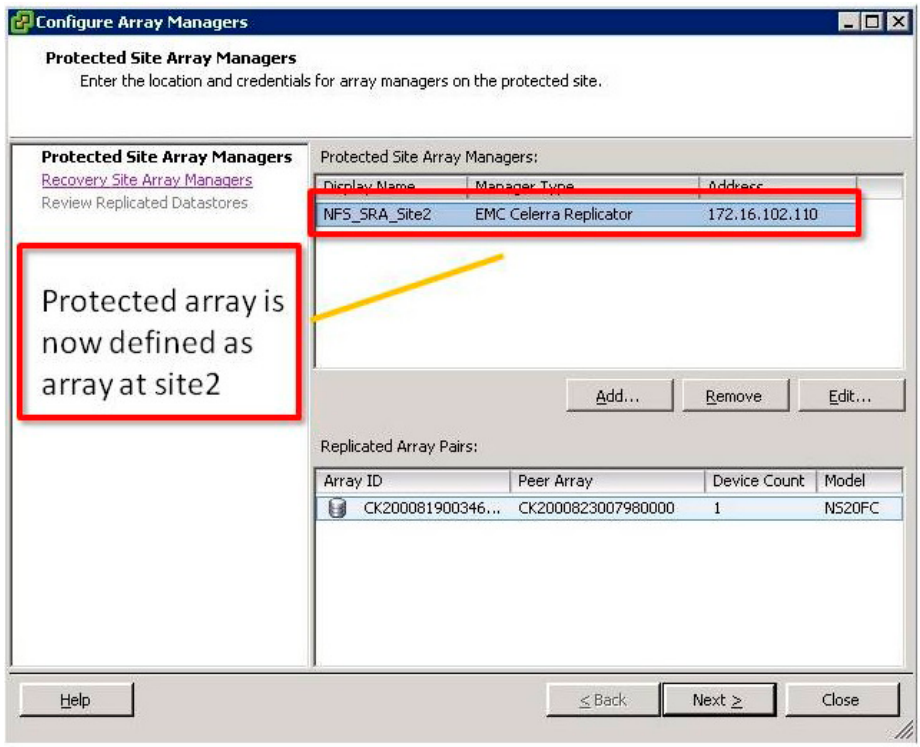


Figure 60 illustrates configuring the recovery site array. The array credentials entered here relate to the storage array that resides in Site 1.

Figure 60: Site 2 recovery site array configuration

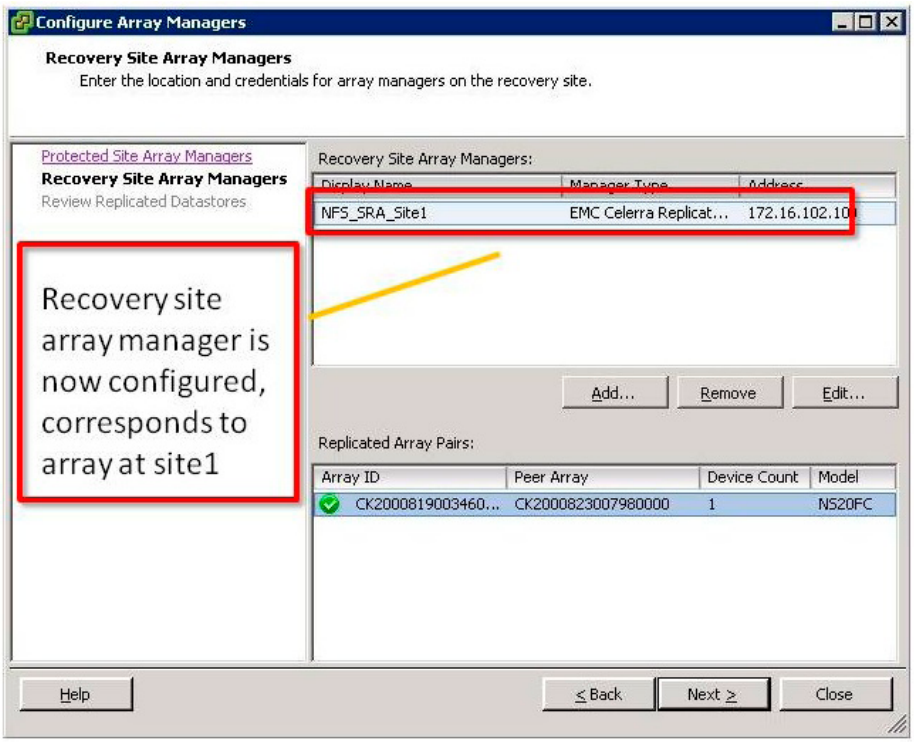
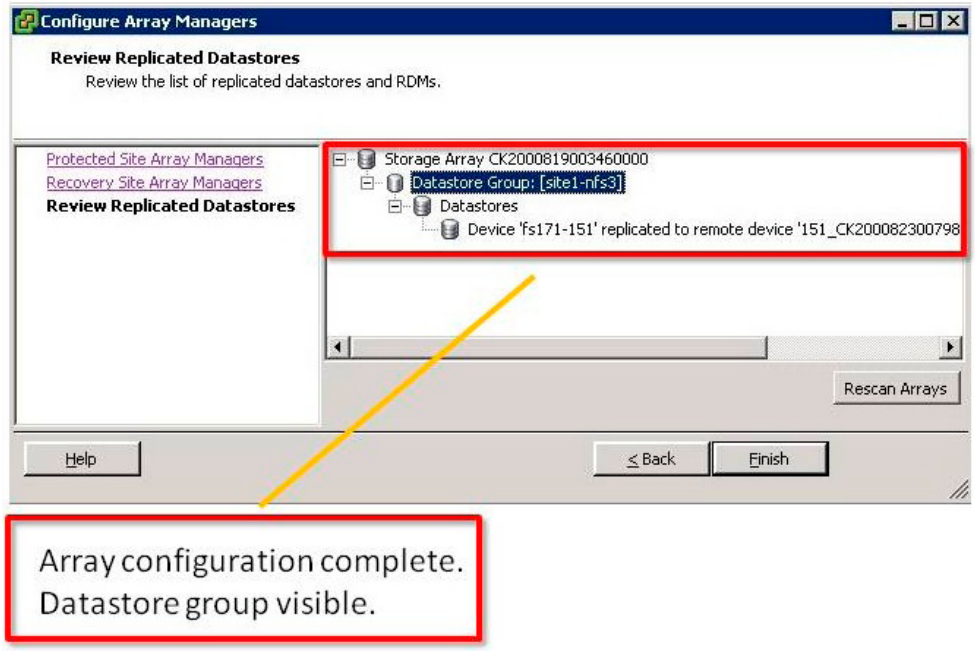


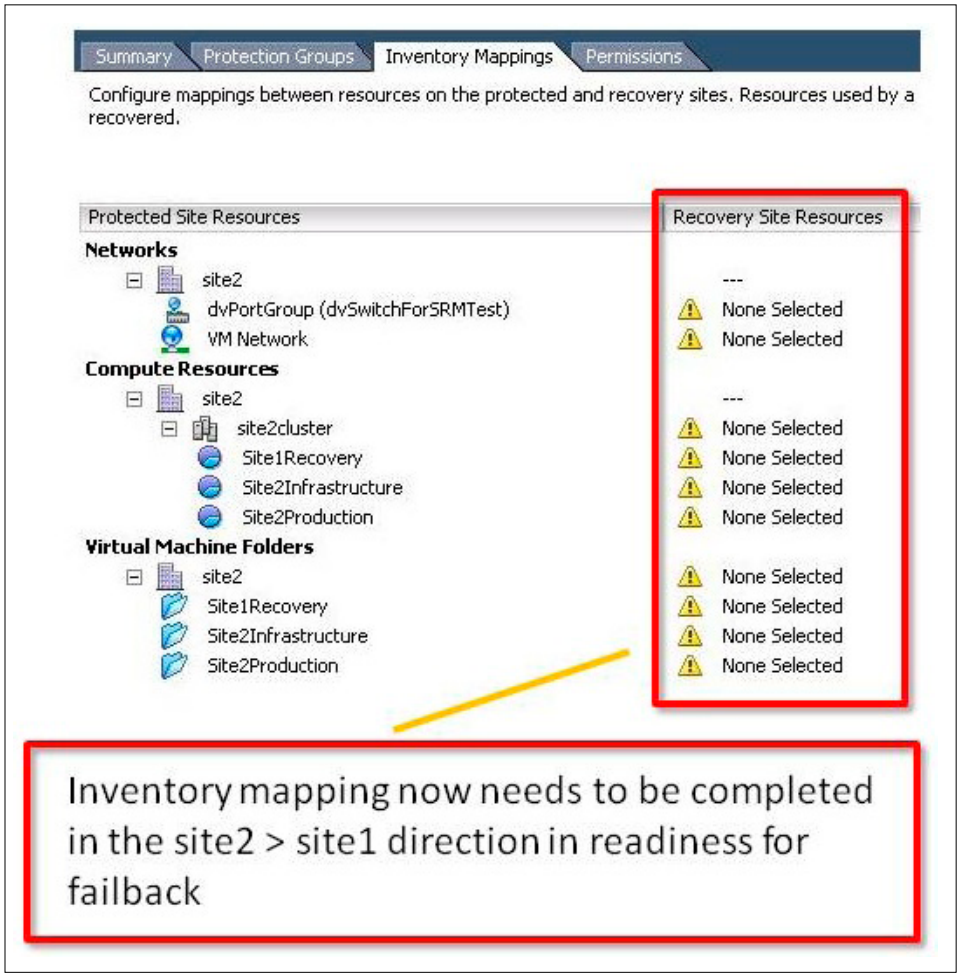
Figure 61 shows the datastore group that relates to the export/datastore that was used to create a new protection group against and ultimately failback to Site 1. The fact that one can see this object is proof that this storage replication reversal was successful. If you do not see any objects at this point the first set of checks to be made in your troubleshooting should verify the storage replication is working as expected in the Site 2 to Site 1 direction.

Figure 61: Site 2 review replicated datastores



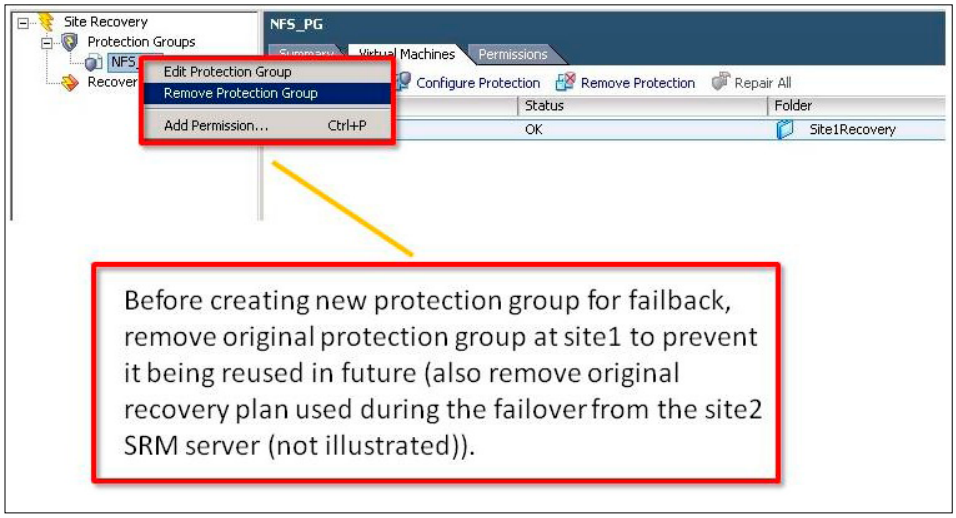
5. **Configure Site Recovery Manager Inventory mapping within Site 2 Site Recovery Manager server**. Other than the array manager configuration, Site Recovery Manager also requires inventory mappings be defined before any protection group can be successfully created. It is highly likely, and shown in this example, that in most configurations the inventory mappings will still be undefined at Site 2. Figure 62 illustrates what most inventory mapping screens will look like at a recovery site Site Recovery Manager server. At this point simply configure the inventory mappings using the same process used to create the mappings at the original protected site.

Figure 62: Site 2 inventory mapping



6. **Remove original protection group at Site 1 and recovery plan at Site 2 used for original virtual machine protection**. After a successful failover the original protection group(s) (Site 1) and recovery plans (Site 2) will still exist. At this time it is good practice to remove these objects to prevent them being re-used accidentally at some later point. First remove the recovery plan at Site 2 used to perform the original failover. Finally remove the protection group from Site 1 as shown in Figure 63.

Figure 63: Site 1 protection group removal

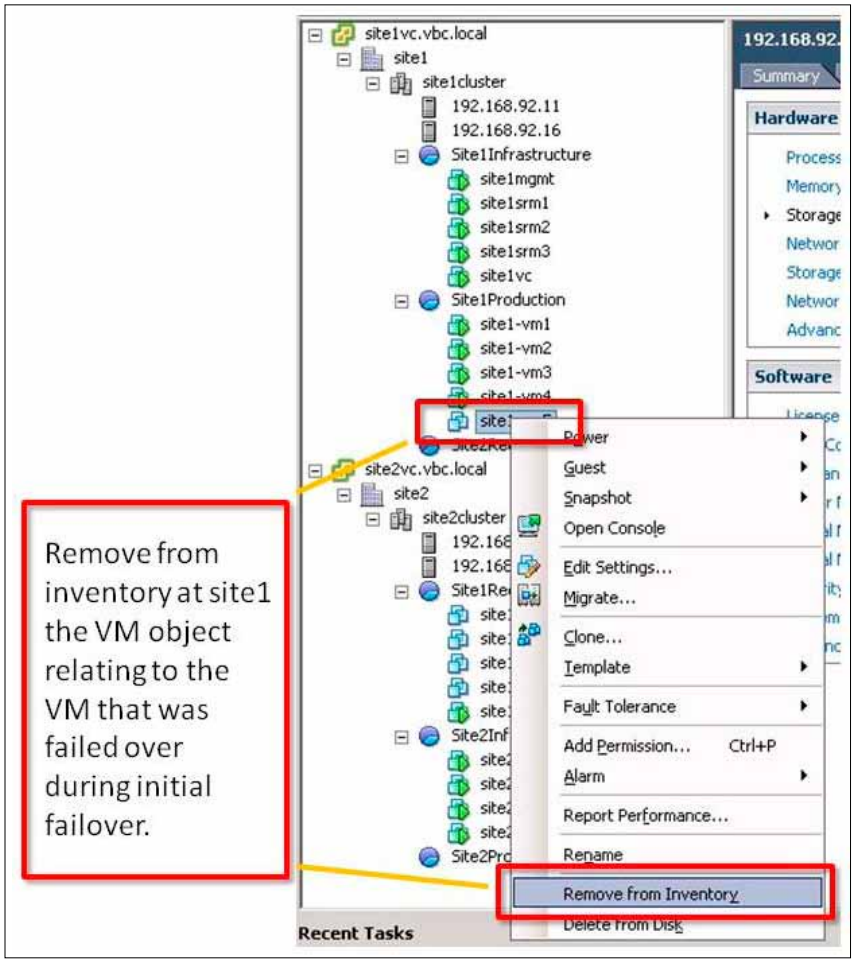


7. **Remove from vCenter inventory virtual machine objects left behind at Site 1 for virtual machines that were failed over to Site 2**. It is almost time to create the new protection group(s) and recovery plan(s). But before that step, the vCenter inventory at Site 1 is reviewed, and you will notice that a virtual machine object still exists for the original virtual machine that was failed over. If you now rescan all ESX hosts at Site 1 (rescan for devices and VMFS volumes) you will see that the virtual machine object grays out, and the word "inaccessible" appears next to it.

   The reason that the virtual machine object grays out is because the storage that object resides on is no longer available in read/write mode as is has been failed over to Site 2 - which means that the copy at Site 2 became read/write. It was then reversed so that the storage replication device at Site 1 is now read/only and hence the virtual machine object is "Inaccessible" at Site 1.

   NOTE: If you are using NFS exports as was done in this example, a rescan will not change the Site 1 virtual machine object state. You can test the device state by simply trying to power the Site 1 virtual machine object on. You will see it will fail. At this point you can un-mount the NFS export(s) from your Site 1 ESX hosts.

Figure 64: Site 1 vCenter inventory cleanup



8. **Create protection group at Site 2 for datastore group containing the NFS export**. Follow the usual steps to create a protection group at Site 2 that maps to the datastore/export you are going to failback.
9. **Create Recovery plan at Site 1 for the protection group created in step 8**. Follow the usual steps to create a recovery plan at Site 1 that maps to the protection group you are going to failback.
10. **Review configuration then test recovery plan using Site Recovery Manager "Test" mode recovery plan functionality**. One of the biggest advantages of using Site Recovery Manager for failback that is often overlooked is the ability to test your failback in the same way as you can test recovery before failing over. The ability to test and re-test failback should be used for every failback operation you perform. Best practice: do not attempt any failback unless a successful test has been performed.

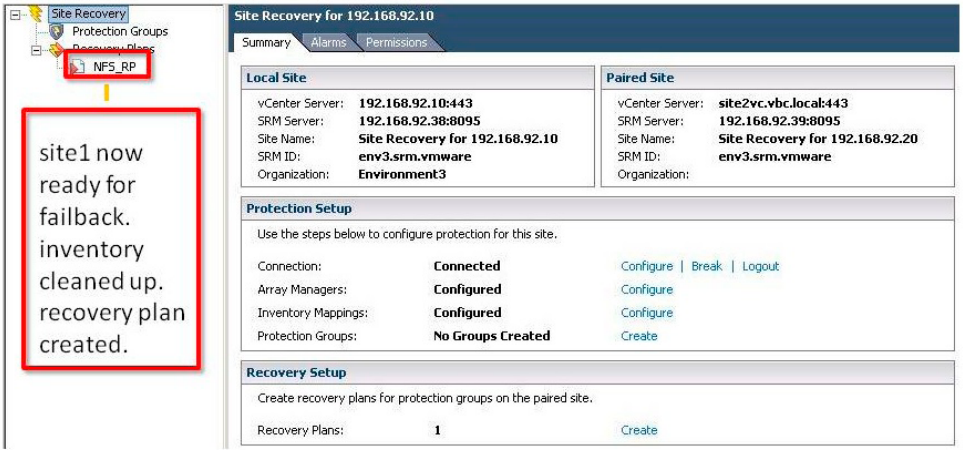
    NOTE: If you wish to test failback prior to actually running the failback check with your storage team that the appropriate functionality is in place on the target storage array to allow the test to take place, this might mean licensing and/or array based snapshot devices.

    Before failback review the configuration of the Site 2 - now the protected site - Site Recovery Manager server and also the Site 1 -now the recovery site - Site Recovery Manager server. At Site 2 you should find that you have a protection group object, configured array manager and inventory mappings as illustrated in Figure 65

Figure 65: Site 2 configuration complete

At Site 1, you should find a recovery plan object as illustrated in Figure 66.

Figure 66: Site 1 configuration complete

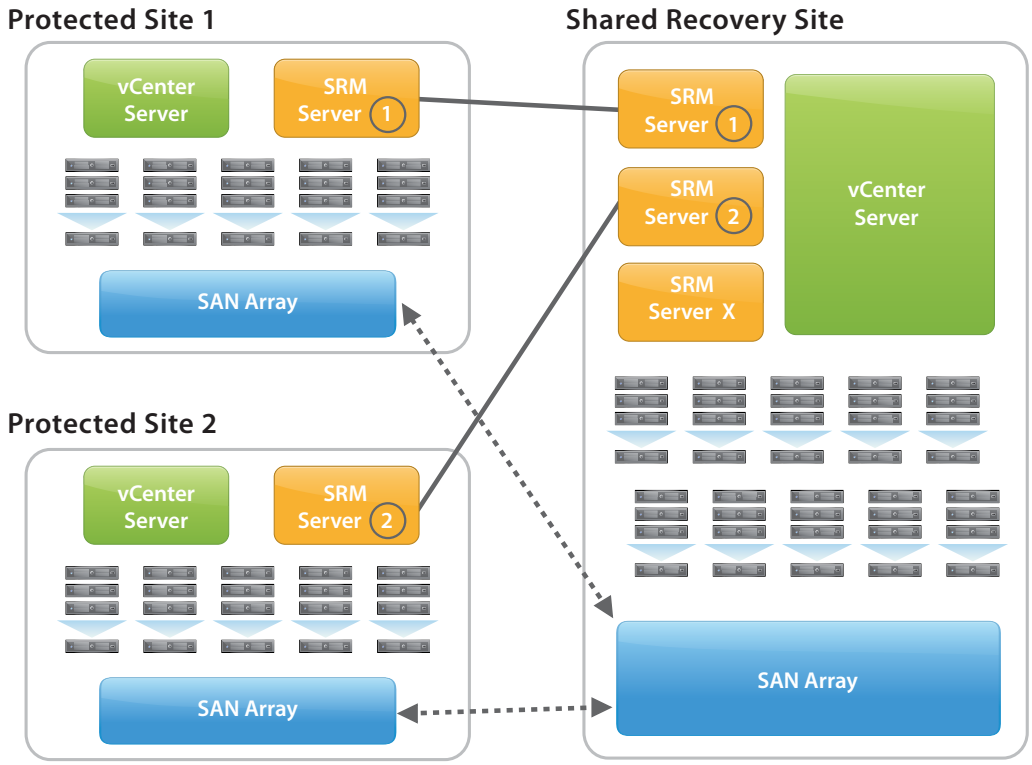


11. **Failback using Site Recovery Manager "Run" mode recovery plan functionality**. Once a successful test has been performed, failback can be carried out by simply running the recovery plan in "**Run**" mode.

7. Shared Recovery Site

Site Recovery Manager 4.0 includes shared recovery site support that enables you to protect virtual machines from multiple vCenter Servers at protected sites to a single vCenter Server at a shared recovery site. In a shared recovery site configuration, you need one instance of vCenter Server on the recovery site and a separate instance of vCenter Server at each of the protected sites. The vCenter Server instance on the recovery site works with the multiple instances of Site Recovery Manager Servers to provide protection to multiple protected sites. Each protected site has its own instance of Site Recovery Manager Server. In this section the use cases of the shared recovery site feature is discussed and details are provided on how to evaluate the feature. See Figure 67.

Figure 67: Shared Recovery Site



NOTE: Pairing a protected site with the shared recovery site requires two important installation configurations.

- Both sites must be installed with the exact same custom Site Recovery Manager extension.
- Both sites must use the same authentication method. If certificate-based authentication is used, both sites must use matching certificates. If credential-based authentication is used, both sites must specify the same values for organization and organization unit.

Overview of Shared Recovery Site Workflow

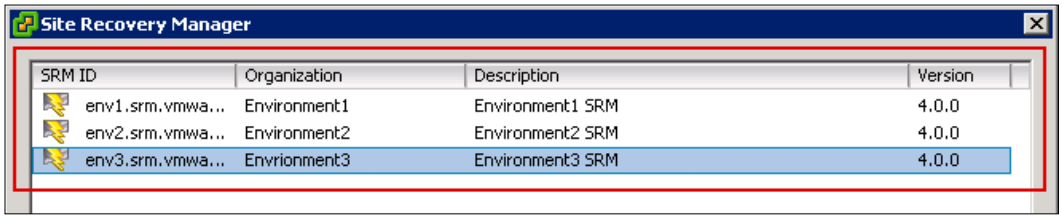
When configured for shared recovery site support, Site Recovery Manager supports the same procedures and workflows that it does in the normal configuration.

- Site Recovery Manager server installation must be initiated from the Windows command shell using a special command-line option. The installation process includes an extra step that specifies a custom

Site Recovery Manager extension name, which is used by a protected site to pair with the matching Site Recovery Manager Server at the shared recovery site.

- Whenever a user connects to the vCenter server at the recovery site and clicks the Site Recovery icon on the vSphere Client Home page, Site Recovery Manager displays a dialog box that requires the user to select a specific Site Recovery Manager extension to connect to.

Figure 68: Select a Site Recovery Manager extension to connect to



Installation

For each shared recovery site customer, you must install Site Recovery Manager once at the customer site and again at the recovery site. Both installations must specify the same custom Site Recovery Manager extension. Each Site Recovery Manager server installation at the shared recovery site must have a dedicated host[12]. You cannot install multiple instances of the Site Recovery Manager server on a single host.

To enable shared recovery site support, run the Site Recovery Manager installer from the Windows command line, as shown in Example 1.

Example 1. Installer Command Line

```
<SRM Installer.exe> /V"CUSTOM_SETUP=1"
```

When run from the command line using this option, the Site Recovery Manager installer presents two additional screens (See Figure 71 and Figure 72) on which you specify a unique Site Recovery Manager extension to be used by a pair of sites.

Click **Custom Site Recovery Manager Plugin identifier**. Any other choice does not support the shared recovery site configuration.

Specify a Custom Site Recovery Manager Extension

The Custom Site Recovery Manager Extension screen presented by the installer has three fields:

- **Site Recovery Manager ID** – a string of up to 20 ASCII characters (80 bytes). The following characters are not allowed: Comma (, ascii 0x2c), Forward slash (/ ascii 0x2f), Backward slash (\ ascii 0x5c), Hash/Pound (# ascii 0x23), Plus (+ ascii 0x2b), Greater (> ascii 0x3e), Lesser (< ascii 0x3c), Equals (= ascii 0x3d), Semi-colon (; ascii 0x3b) and Double quote (" ascii 0x22), and all control characters.
- **Organization** – a string of up to 20 ASCII characters (80 bytes) that specifies the organization owning the extension.
- **Description** – a string of up to 20 ASCII characters (80 bytes) that provides a description of the extension.

[12] The host in reference is a physical machine or a virtual machine, not an ESX Server host.

7.1. Use Cases of Shared Recovery Site

With the shared recovery site feature, organizations can use Site Recovery Manager to accommodate use cases in which multiple protected sites are configured to failover to a single recovery site. These organizations include:

1. ROBO: Enterprise companies that have many remote field offices can protect their remote offices by a centralized recovery site. See Figure 69.
2. Disaster Recovery Hosting: DR Service Providers that have a data center that can be used to protect the virtual environments of multiple customers. See Figure 70.

Figure 69: Shared Recovery Site – ROBO Protection

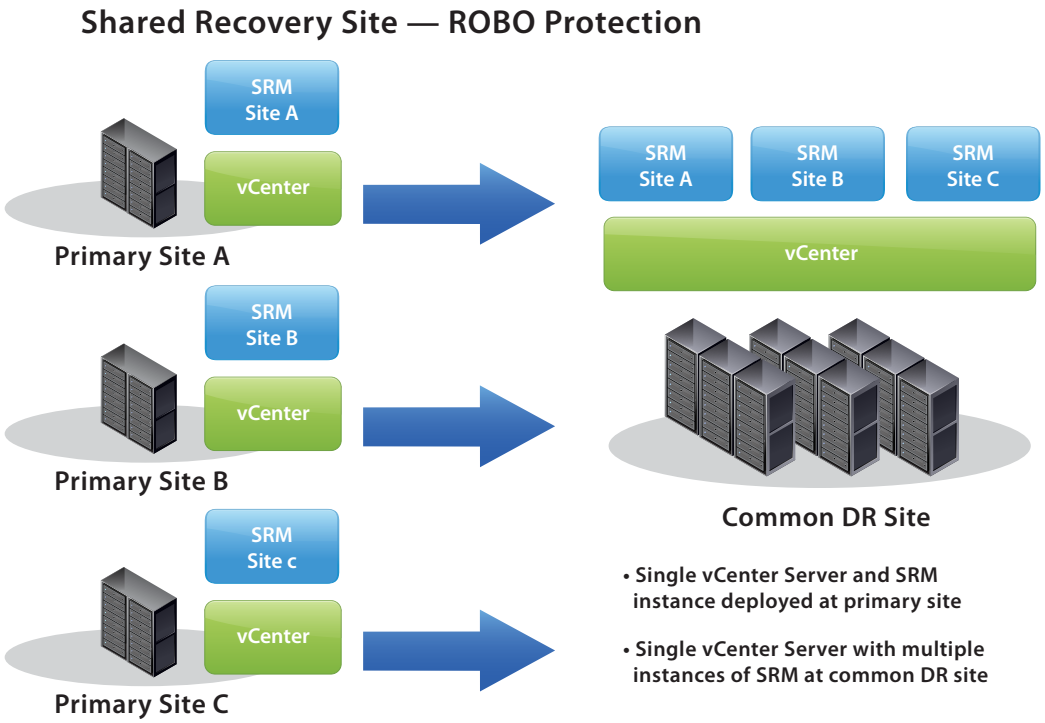
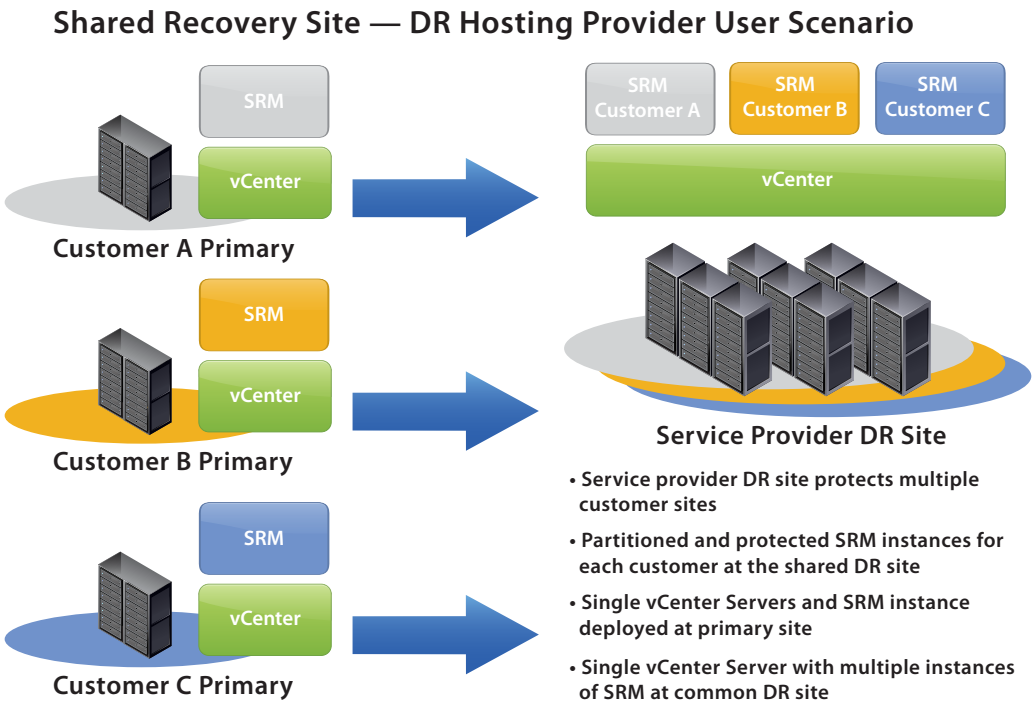


Figure 70: Shared Recovery Site – DR Hosting Provider Use Scenario


Shared Recovery Site — DR Hosting Provider User Scenario
SRM
vCenter
Customer A Primary
SRM
vCenter
Customer B Primary
SRM
vCenter
Customer C Primary
SRM Customer A
SRM Customer B
SRM Customer C
vCenter
Service Provider DR Site
• Service provider DR site protects multiple customer sites
• Partitioned and protected SRM instances for each customer at the shared DR site
• Single vCenter Servers and SRM instance deployed at primary site
• Single vCenter Server with multiple instances of SRM at common DR site

7.2. Optional Exercise: Configuring Shared Recovery Site

Shared Recovery Site	**Configure Shared Recovery Site**	Protect 2 sites by a shared recovery site Pre-requisite: Two protected sites with separate vCenter servers, one recovery site with another vCenter server. 1. Install a SRM instance using a custom switch on both the protected and recovery sites with custom SRM plug-in ID and same authentication method. 2. Pair sites. 3. Install a SRM instance on another protected site and another SRM instance on the recovery site. Repeat the procedures in step 1 and step 2.	20 minutes

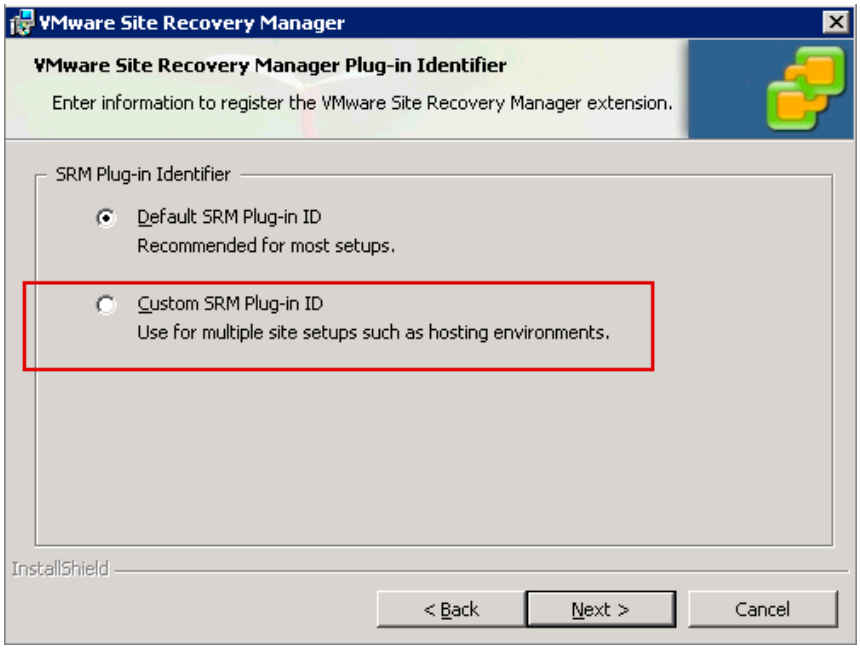
Step 1: Install a Site Recovery Manager instance using a custom switch on both the protected and recovery sites with custom Site Recovery Manager plug-in ID and same authentication method.

Procedure:

On protected site

1. Install Site Recovery Manager using the switch `/V"CUSTOM_SETUP=1"`
2. During the installation, you will be prompted to enter a Default Site Recovery Manager Plug-in ID or a Custom Site Recovery Manager Plug-in ID. Choose **Custom Site Recovery Manager Plug-in ID**.

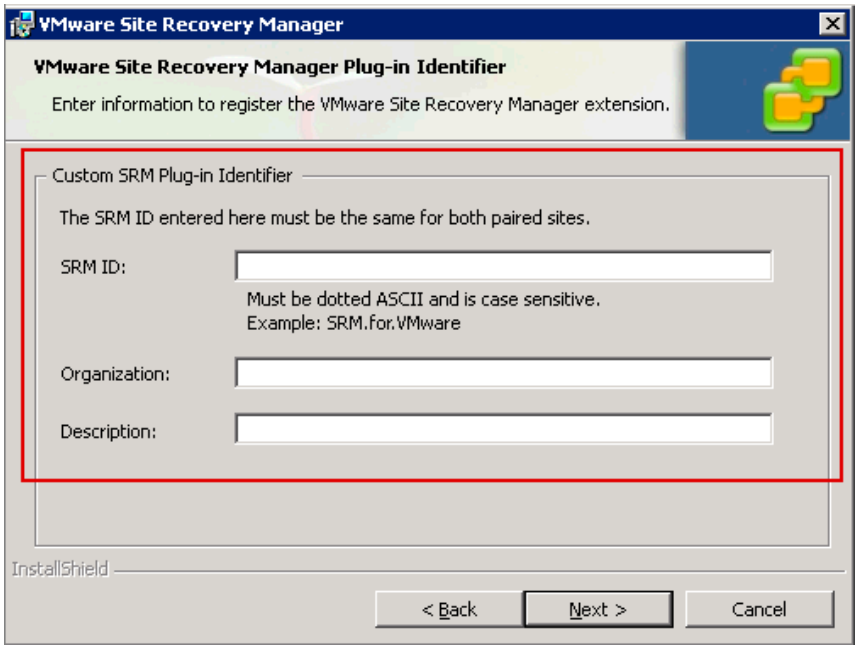
Figure 71: Select Custom Site Recovery Manager Plug-in ID


VMware Site Recovery Manager
VMware Site Recovery Manager Plug-in Identifier
Enter information to register the VMware Site Recovery Manager extension.
SRM Plug-in Identifier
Default SRM Plug-in ID
Recommended for most setups.
Custom SRM Plug-in ID
Use for multiple site setups such as hosting environments.
InstallShield
< Back
Next >
Cancel

3. Enter the Custom Site Recovery Manager Plug-in ID:

SRM ID	env1.srm.vmware
ORGANIZATION	Environment1
ORGANIZATION	Protected Site for Environment 1 in a shared recovery site configuration

Figure 72: Enter custom Site Recovery Manager Plug-in ID


VMware Site Recovery Manager
VMware Site Recovery Manager Plug-in Identifier
Enter information to register the VMware Site Recovery Manager extension.
Custom SRM Plug-in Identifier
The SRM ID entered here must be the same for both paired sites.
SRM ID:
Must be dotted ASCII and is case sensitive.
Example: SRM.for.VMware
Organization:
Description:
InstallShield
< Back
Next >
Cancel

On recovery site

1. Install Site Recovery Manager using the switch `/V"CUSTOM_SETUP=1"`
2. During the installation, you will be prompted to enter a Default Site Recovery Manager Plug-in ID or a Custom Site Recovery Manager Plug-in ID. Choose **Custom Site Recovery Manager Plug-in ID**.
3. Enter the Custom Site Recovery Manager Plug-in ID:

SRM ID	env1.srm.vmware
ORGANIZATION	Environment1
ORGANIZATION	Recovery Site for Environment 1 in a shared recovery site configuration

NOTE: Both sites must use the same authentication method. If certificate-based authentication is used, both sites must use matching certificates. If credential-based authentication is used, both sites must specify the same values for organization and organization unit.

Step 2: Pair sites

Follow the procedure to pair sites specified in section 1.

Step 3: Install a Site Recovery Manager instance on another protected site and another Site Recovery Manager instance on the recovery site.

Repeat the procedures in step 1 and step 2 and use a different Site Recovery Manager Custom ID for this installation:

1. Enter the Custom Site Recovery Manager Plug-in ID for the Site Recovery Manager Server instance on the protected site:

SRM ID	env2.srm.vmware
ORGANIZATION	Environment2
DESCRIPTION	Protected Site for Environment 2 in a shared recovery site configuration

2. Enter the Custom Site Recovery Manager Plug-in ID for the Site Recovery Manager Server instance on the recovery site:

SRM ID	env2.srm.vmware
ORGANIZATION	Environment2
DESCRIPTION	Recovery Site for Environment 2 in a shared recovery site configuration

After these 3 steps, you will have an environment with two sites being protected by one recovery site. The recovery site has 2 Site Recovery Manager Server instances and 1 vCenter Server instance and the protected sites have 1 Site Recovery Manager Server instance and 1 vCenter Server instance each.

8. Conclusion

VMware vCenter Site Recovery Manager (SRM) leverages your VMware vCenter and vSphere platform to make disaster recovery:

- **Rapid** - by automating the disaster recovery process for your virtual machines by eliminating the complexities of traditional physical disaster recovery.
- **Reliable** - by ensuring proper execution of the recovery plan as well as the ability to enable easier, more frequent tests in an isolated environment without impacting services in the protected site.
- **Manageable** - centrally manage recovery plans and make plans dynamic to match a dynamic virtualized environment.
- **Affordable** - utilize recovery site infrastructure and reduce management costs.

Site Recovery Manager enables you to:

- **Expand disaster recovery protection** - now any workload in a virtual machine can be protected with minimal incremental effort and cost.
- **Reduce time to recovery** - as soon as a disaster is declared, Site Recovery Manager allows for the recovery of protected virtual machines with a few mouse clicks to the designated recovery site.
- **Increase reliability of recovery** - replication of system state ensures your protected virtual machines have all they need to startup in the protected site. Hardware independence that is realized through your VMware Infrastructure eliminates failures due to different hardware.
- **Easier and more frequent testing** – Site Recovery Manager enables you to test your recovery plan in an isolated environment without impacting services in the protected site while using the actual failover sequence that will be executed during a real disaster.

Site Recovery Manager 4.0 provides additional features – vSphere support, NFS support and support for multiple-to-one shared recovery site, which you can leverage to extend your disaster recovery plan to cover even more of your disaster recovery needs.

This guide provides you with step-by-step instructions on how to setup automated disaster recovery workflows using Site Recovery Manager as well as other cutting-edge DR features in Site Recovery Manager. With Site Recovery Manager you can design and implement a comprehensive disaster recovery plan for your virtual environment. After going through the evaluation exercises in this guide, you should be able to make the right choice to implement your disaster recovery solutions in your virtual datacenter.

VMware vCenter Site Recovery Manager 4.0 Evaluator's Guide
Source: Technical Marketing, DC, LD
Revision: 200901001

vmware®

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMW_09Q3_SRM_EG_EN_P65_R1

vmware®